Preuve et services de confiance dans l'environnement numérique

Jacquemin, Hervé

Published in:
Pas de droit sans technologie

Publication date:
2015

Document Version
le PDF de l'éditeur

2

PREUVE ET SERVICES DE CONFIANCE DANS L'ENVIRONNEMENT NUMÉRIQUE

Hervé Jacquemin
chargé d'enseignement à l'UNamur (CRIDS)
chargé de cours invité à l'U.C.L. et à l'ICHEC
avocat

Sommaire

Introduction

1. Preuve et environnement numérique. Pour souligner l'importance pratique des règles de preuve, l'adage *idem est non esse aut non probari* est généralement rappelé. Il signifie qu'à défaut de preuve valable, si un litige survient, il sera extrêmement difficile à la partie sur laquelle repose la charge de la preuve[1] de faire valoir ses droits[2]. Aussi pourrait-elle perdre le procès, avec les conséquences potentiellement négatives qui en résultent. Le principe s'applique tant en matière civile qu'en matière commerciale même si le principe de la liberté de la preuve[3], applicable dans ce dernier cas, tend à réduire l'irrecevabilité des présomptions et des témoignages (risque réel en matière civile, avec la prééminence de l'écrit[4])[5].

Les technologies de l'information et de la communication constituent désormais une réalité quotidienne, notamment en matière contractuelle. Les contrats imprimés sur le papier, au bas desquels chaque partie appose sa signature manuscrite, sont ainsi remplacés, de plus en plus souvent, par des documents électroniques, transmis par courriels et munis – mais très rarement – d'une signature électronique. On constate aussi une volonté certaine des entreprises ou des autorités publiques d'aller vers davantage de dématérialisation, pour simplifier les procédures et diminuer les coûts de traitement et de conservation.

Les règles relatives au fardeau de la preuve s'appliquant également dans l'environnement numérique, il incombe à la partie désignée par celles-ci de respecter scrupuleusement les exigences probatoires. S'agissant principalement de règles de forme (signature, écrit, mentions manuscrites, exemplaires multiples, etc.), la difficulté consiste à les accomplir valablement dans l'environnement numérique, étant entendu qu'elles ont principalement été conçues dans un environnement « papier ».

1. Conformément à l'article 1315 du C. civ. et à l'article 870 du C. jud.
2. Pour F. Gény, « l'existence juridique d'un fait dépend tellement de sa preuve, que celle-ci en reste la première condition d'efficacité » (F. Gény, *Science et technique en droit privé positif*, t. III, Paris, Sirey, 1921, p. 110, n° 205). H. De Page note aussi que « la preuve est, dans son principe, de nécessité absolue en droit. Ce qui n'est pas prouvé n'est pas affecté, pour cela, dans son existence, sans doute, mais est pratiquement privé de toute utilité, est frappé de stérilité » (De Page, *Traité élémentaire de droit civil belge*, t. III, 3e éd., Bruxelles, Bruylant, 1967, p. 695, n° 707). Voy. aussi J. Dabin, « La technique de la preuve juridique, spécialement en droit civil », *B.J.*, 1932, col. 353; R. Legeais, *Les règles de preuve en droit civil. Permanences et transformations*, Paris, Librairie Générale de Droit et de Jurisprudence, 1955, p. 49; A. Colin et H. Capitant, *Traité de droit civil*, (refondu par L. Julliot de la Morandière), t. 2, Paris, Dalloz, 1959, t. 2, p. 350, n° 620; P. Catala, « Le formalisme et les nouvelles technologies », *Rép. Defrénois*, 2000, p. 899, n° 4; Ph. Malinvaud, « L'impossibilité de la preuve écrite », *J.C.P.*, 1972, I (n° 2468), n° 3; M. Van Quickenborne, « Quelques réflexions sur la signature des actes sous seing privé », note sous Cass., 28 juin 1982, *R.C.J.B.*, 1985, p. 70, n° 5; P. Wéry, D. Gobert et L. Kerzmann, « La preuve », *Guide juridique de l'entreprise*, 2e éd., Bruxelles, Kluwer, 2003, p. 20, n° 160.
3. Art. 25, al. 1er, C. comm.
4. Art. 1341 C. civ.
5. Sur la différence entre les règles de preuve en matière civile et commerciale, voy. H. Jacquemin et L. Kerzmann, « La preuve en matière commerciale », *La preuve au carrefour de cinq disciplines juridiques*, Limal, Anthemis, 2013, pp. 79-108.

2. Interventions législatives précoces. Dans ce domaine, le législateur est intervenu très – sans doute même trop – tôt en vue de lever les obstacles formels. Au niveau international, on se rappelle ainsi des lois-types de la CNUDCI sur le commerce électronique (1996) et sur la signature électronique (2001)[6], ainsi que des directives européennes sur la signature électronique[7] (1999) et sur le commerce électronique[8] (2000).

En droit belge, les principales dispositions légales sont en vigueur depuis le début des années 2000. Pour la signature, il faut principalement avoir égard à l'article 1322, alinéa 2, du Code civil[9] et à la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électronique et les services de certification[10] (qui transposent la directive sur la signature électronique). Quant aux autres obstacles formels, ils étaient visés par les articles 16 et 17 de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information[11] (LSSI), désormais intégrés dans le livre XII du Code de droit économique (art. XII.15 et XII.16).

3. Règlement eIDAS. Les mérites de ces textes sont indéniables. À l'analyse, on doit toutefois constater que, s'agissant spécialement de la signature électronique, rares sont les procédés utilisés en pratique qui respectent les exigences présentant le plus haut niveau de sécurité juridique et technique (sans que cela pose de réelles difficultés dans la vie des affaires).

En outre, il restait de nombreuses incertitudes pour diverses formalités, sans doute accessoires, mais néanmoins cruciales en pratique: on songe à l'horodatage, au recommandé ou à l'archivage électroniques,

6. On peut également ajouter la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (2005). Ces textes sont disponibles sur le site web de la CNUDCI (www.uncitral.org).
7. Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, *J.O.*, L 13 du 19 janvier 2000.
8. Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), *J.O.*, L 178 du 17 juillet 2000.
9. Cet alinéa 2 a été ajouté par l'art. 2 de la loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 décembre 2000.
10. *M.B.*, 29 septembre 2001.
11. *M.B.*, 17 mars 2003.

pour lesquels le cadre normatif était, en droit de l'Union et en droit belge, inexistant ou, à tout le moins, totalement insuffisant.

Le législateur européen y a vu un obstacle à l'instauration d'un climat de confiance dans l'environnement numérique. Or, sans cette indispensable confiance, les consommateurs, les entreprises ou les autorités publiques hésiteront sans doute à réaliser des transactions en ligne, se privant ainsi du potentiel de croissance et de développement économique que constitue le recours aux technologies de l'information et de la communication.

Aussi la Commission a-t-elle pris l'initiative et déposé une proposition de règlement en juin 2012[12]. Le texte a été adopté près de deux ans plus tard : il s'agit du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE[13] (ci-après, « règlement eIDAS »)[14].

4. Objet et plan de la présente contribution. Après un bref rappel des principales dispositions légales ou réglementaires et de leur domaine d'application respectif (*infra*, sect. 1), nous examinons les enjeux d'une réglementation dans le domaine de la preuve et des services de confiance (*infra*, sect. 2). Tenant compte de ces considérations, nous analysons ensuite de quelle manière le législateur (européen et belge) est intervenu pour y répondre efficacement (*infra*, sect. 3).

Jusqu'à l'adoption récente du règlement eIDAS, le cadre normatif n'avait pas évolué de manière significative, la jurisprudence restant par ailleurs assez rare. Aussi nous focaliserons-nous sur le nouveau régime introduit par le règlement eIDAS en matière de services de confiance[15], renvoyant pour le surplus à la littérature consacrée aux dispositions actuellement en vigueur[16].

12. Proposition de règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, 4 juin 2012, COM (2012) 238 final.
13. *J.O.*, L 257 du 28 août 2014.
14. Pour une première analyse du règlement, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : évolution ou révolution », *R.D.T.I.*, 2014/56, pp. 27 et s.
15. Nous ne traitons pas des aspects liés à l'identification électronique.
16. Pour des études récentes, voy. E. MONTERO, « La preuve des actes juridiques privés électroniques en droit belge », *R.L.D.I.*, 2009, pp. 19-26 ; P. VAN EECKE, « De elektronische handtekening in het recht », *R.D.C.*, 2009, pp. 323-354 ; H. JACQUEMIN, *Le formalisme contractuel. Mécanisme de protection de la partie faible*, Bruxelles, Larcier, 2010, pp. 327 et s., n^{os} 242 et s. ; E. MONTERO et H. JACQUEMIN, « Commerce électronique et contrats de l'informatique », *Chronique de jurisprudence en droit des technologies de l'information (2009-2011)*, *R.D.T.I.*, 2012/48-49, pp. 5-28 ; D. MOUGENOT, « La preuve et les nouvelles technologies », *La preuve au carrefour de cinq disciplines juridiques*, Limal, Anthemis, 2013, pp. 161 et s.

Précisons encore que seuls les aspects de droit privé de la preuve numérique sont pris en compte.

Section 1

Champ d'application des principales dispositions légales ou réglementaires

5. Complexité du cadre normatif. Les dispositions légales ou réglementaires susceptibles d'être invoquées au moment de faire la preuve de ses droits dans l'environnement numérique forment un cadre normatif relativement complexe[17].

D'une part, il faut articuler des règles dont les domaines d'application respectifs se croisent sans coïncider parfaitement. En outre, il faut être attentif à l'existence, dans certains cas, d'une disposition spéciale qui déroge à la loi générale et s'applique par priorité à celle-ci. On le verra notamment s'agissant de la signature ou des autres formalités (*infra*, n° 7).

D'autre part, dès que le règlement eIDAS sera d'application (le 1er juillet 2016, pour la plupart des dispositions), il conviendra de l'articuler avec les dispositions prises en droit belge en matière de signature ou d'autres services de confiance, que ce soit au niveau fédéral ou des entités fédérées.

Dans cette contribution, on examinera principalement la clause transversale générale et les clauses transversales particulières de l'article XII.15 du Code de droit économique, la législation belge en matière de signature électronique et le règlement eIDAS (*infra*, n^{os} 6 et s.).

Pour mémoire, on se souviendra que le législateur belge a déjà eu la volonté de réguler les services de confiance.

Une loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance[18] a ainsi été adoptée, pour encadrer les activités des prestataires de service d'archivage électronique, d'horodatage électronique, de recommandé électronique et de blocage transitoire

17. Il faut également avoir égard aux dispositions conventionnelles qui ont été prises par les parties. On sait, en effet, que le droit commun de la preuve n'est ni d'ordre public, ni impératif. Par conséquent, les parties peuvent valablement déroger aux exigences – de forme, en particulier – prévues dans ce cadre, en déclarant recevable et en donnant valeur probante à un procédé de signature électronique qui, par exemple, ne respecterait pas nécessairement les conditions de l'article 1322, alinéa 2, du Code civil ou de l'article 4, § 4, de la loi du 9 juillet 2001 (le cas échéant, la validité de ces clauses peut être appréciée à la lumière des dispositions du livre VI du Code de droit économique, qui régissent les clauses abusives, not. l'art. VI.83, 21°, qui considère abusive la clause qui « limite les moyens de preuve que le consommateur peut utiliser »).
18. *M.B.*, 17 juillet 2007.

des sommes versées. Diverses obligations, assez générales, sont imposées à ces prestataires. Elles portent sur leur impartialité (art. 4), leur attitude vis-à-vis des données qui leur sont transmises (art. 5), les mesures de sécurité à mettre en œuvre (art. 6), les informations à communiquer aux destinataires de leurs services (art. 7), la compétence de leur personnel (art. 8), la confidentialité (art. 9) et leur capacité financière (art. 10). Pour le surplus, la loi donne délégation au Roi pour déterminer, par arrêté délibéré en conseil des ministres, les obligations spécifiques auxquelles sont soumis chacun des prestataires visés par la loi (art. 16, al. 1er, 1°). L'article 16 impose au Roi d'intervenir jusqu'au 1er décembre 2007 au plus tard. Il apparaît cependant qu'il n'est pas intervenu. Il faut donc en conclure qu'en l'absence de régime spécifique applicable, l'activité de ces prestataires n'est pas légalement encadrée, ce qui rend la loi parfaitement inutile.

Plus récemment, les services d'archivage, d'horodatage et de recommandé électroniques ont également fait l'objet d'une proposition de loi[19]. Elle vise à introduire dans le livre XII du C.D.E. (intitulé « droit de l'économie électronique ») un titre 2 reprenant les dispositions de la loi du 9 juillet 2001 et de nouvelles dispositions sur ces trois services de confiance. Dans le cadre de la procédure instaurée par la directive « transparence »[20], le texte avait été bloqué par la Commission jusqu'en octobre 2014 (tenant compte de l'adoption prévue du règlement eIDAS), soit après les élections législatives de mai 2014. Aussi la proposition est-elle devenue caduque[21].

6. Article XII.15 du Code de droit économique. L'article XII.15 du C.D.E. consacre la théorie des équivalents fonctionnels (§ 1er) et l'applique à trois formalités (§ 2) : l'écrit, la signature et la mention manuscrite.

En pratique, cette disposition présente un grand intérêt puisqu'elle permet de lever la plupart des obstacles formels.

19. Proposition de loi du 15 avril 2013 modifiant la législation en ce qui concerne l'instauration du droit de l'économie électronique, *Doc. parl.*, Ch. repr., sess. ord. 2012-2013, n° 2745/001. Voy. aussi l'amendement du Gouvernement visant à compléter la proposition de loi portant insertion d'un titre 2, 'Certaines règles relatives au cadre juridique pour les signatures électroniques, l'archivage électronique, le recommandé électronique, l'horodatage électronique et les services de certification', dans le livre XII du Code de droit économique, et portant insertion des définitions propres au titre 2 précité et des dispositions d'application de la loi propres au même titre, dans les livres I et XV du Code de droit économique, *Doc. parl.*, Ch. repr., sess. ord. 2012-2013, n° 2745/004.
20. Directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information, *J.O.*, L 204 du 21 juillet 1998.
21. Il est toutefois hautement probable qu'elle serve de modèle au législateur belge pour amender – lorsque cela s'avère nécessaire – le cadre normatif actuellement en vigueur à l'aune du règlement eIDAS.

Encore faut-il que l'exigence de forme entre dans le champ d'application de cette disposition.

D'un point de vue positif, il doit s'agir d'une exigence légale ou réglementaire de forme relative au processus contractuel[22] et qu'il convient d'accomplir dans le cadre d'un service de la société de l'information[23].

D'un point de vue négatif, il faut exclure les matières visées à l'article XII.1, § 2 (fiscalité, vie privée et traitement des données à caractère personnel, droit des ententes, etc.), et les contrats relevant des catégories listées à l'article XII.16, parmi lesquels figurent notamment les « contrats qui créent ou transfèrent des droits sur des biens immobiliers, à l'exception des droits de location » ou « les contrats de sûretés et garanties fournis par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale ».

7. Législation belge en matière de signature électronique. Pour transposer la directive sur la signature électronique de 1999, le législateur belge a, d'une part, ajouté un second alinéa à l'article 1322 du Code civil, d'autre part, adopté la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (ci-après, la loi du 9 juillet 2001). Par la suite, d'autres dispositions spécifiques traitant de la signature électronique ont aussi été adoptées. On songe par exemple à l'article 3*bis* de la loi du 3 juillet 1978 relative au contrat de travail.

Il importe de saisir correctement le domaine d'application de ces dispositions et de comprendre la manière de les articuler. À cet égard, une distinction doit être faite entre les signatures requises dans une perspective probatoire, et dont l'unique objectif est de garantir la sécurité des relations contractuelles en offrant aux parties un moyen de preuve efficace, d'une part, et celles qui peuvent poursuivre d'autres objectifs, par exemple protéger l'un des cocontractants supposé en position de faiblesse, d'autre part[24]. On note que, selon le cas, la sanction susceptible d'être prononcée en cas d'inobservation de la formalité est différente. Dans le premier cas, l'absence de signature a pour conséquence de rendre l'acte juridique plus difficile, voire impossible à prouver, alors que dans le second, sa validité sera affectée et il pourra être annulé ou converti.

22. Art. XII.15, § 1er, du C.D.E.
23. Voy. l'art. XII.1, § 2, du C.D.E., suivant lequel « le présent titre règle certains aspects juridiques des services de la société de l'information ». On pourrait toutefois soutenir une position différente dans la mesure où, contrairement aux autres dispositions du titre 1er, du livre XII du C.D.E., qui concernent l'information et de la transparence sur les réseaux, la publicité et la responsabilité des prestataires intermédiaires, les notions de « service de la société de l'information », de « prestataire » ou de « destinataire de service », n'apparaissent pas à l'article XII.15.
24. À ce sujet, voy. H. JACQUEMIN, *Le formalisme contractuel. Mécanisme de protection de la partie faible*, *op. cit.*, n°s 173 et s.

La prudence recommande de limiter l'application de l'article 1322, alinéa 2, du Code civil, qui traite de la signature électronique, au droit de la preuve[25], plus précisément à la signature des actes sous seing privé, requise conformément à l'article 1341 du même Code.

La section 2 du chapitre II de la loi du 9 juillet 2001, intitulée « champ d'application », est composée d'un article unique aux termes duquel « la présente loi fixe certaines règles relatives au cadre juridique pour les signatures électroniques et définit le régime juridique applicable aux opérations effectuées par les prestataires de service de certification ainsi que les règles à respecter par ces derniers et les titulaires de certificats sans préjudice des dispositions légales concernant les règles de représentations des personnes morales [...] ». *A priori*, la loi ne limite pas son application, *ratione materiae*, à certains rapports contractuels, ou, *ratione personae*, à certaines catégories de cocontractants. On peut se demander si, à l'instar de l'article 1322, alinéa 2, du Code civil, la loi vise uniquement la signature requise dans une perspective probatoire. En analysant la loi de manière générale, la réponse est négative[26-27].

25. On peut se fonder sur la place qu'il occupe dans le Code civil (l'art. 1322 est en effet inséré dans le livre III, titre III, chapitre VI, intitulé « De la preuve des obligations et de celle du paiement ») et sur le contexte d'adoption de la loi (voy. spéc. l'avis du Conseil d'État, *Doc. parl.*, Ch. repr., sess ord. 1998-1999, n° 49-2141/001, p. 27, et l'introduction de l'expression « pour l'application du présent article »). En ce sens, voy. M. DEMOULIN et E. MONTERO, « Le formalisme contractuel à l'heure du commerce électronique », *Commerce électronique: de la théorie à la pratique*, Cahier du CRID, n° 23, Bruxelles, Bruylant, 2003, p. 184 (la « réforme n'affecte pas, en principe, les situations où une signature manuscrite est requise pour la validité d'un acte juridique ou son opposabilité aux tiers »); P. LECOCQ et B. VANBRABANT, « La preuve du contrat conclu par voie électronique », *Le commerce électronique: un nouveau mode de contracter*, Liège, Éd. du Jeune Barreau, 2001, p. 127, n° 116; J. DUMORTIER et S. VAN DEN EYNDE, « De juridische erkenning van de elektronische handtekening in België », *Computerr.*, 2001, p. 188; D. MOUGENOT, *La preuve*, 3e éd., tiré à part du *Rép. not.*, Bruxelles, Larcier, 2002, p. 190, n° 122-3; L. GUINOTTE, « La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001 », *J.T.*, 2002, p. 558.
26. M. DEMOULIN et E. MONTERO, « Le formalisme contractuel à l'heure du commerce électronique », *op. cit.*, p. 186.
27. La lettre des dispositions-clés de la loi, qui énoncent les principes d'assimilation (art. 4, § 4) et de non-discrimination (art. 4, § 5), pourrait cependant instiller le doute. Le principe d'assimilation est établi, aux termes de l'article 4, § 4, « sans préjudice des articles 1323 et suivants du Code civil [...] », relatifs à la contestation de signature et d'écriture, en matière probatoire essentiellement. Quant à l'article 4, § 5, il dispose qu'« une signature électronique ne peut être privée de son efficacité juridique et ne peut être *refusée comme preuve en justice* au seul motif [...] » (nous soulignons). Si le doute existe, il n'emporte toutefois pas notre conviction. Rien n'empêche de contester une signature conformément aux règles des articles 1323 et suivants du Code civil lorsque celle-ci n'est pas requise uniquement dans une perspective probatoire. Quant au refus de la signature comme preuve en justice, il peut être considéré comme une application particulière de l'inefficacité juridique, qui recouvre également d'autres sanctions (la nullité de l'acte juridique pour défaut de signature, par exemple). Considérant que, nonobstant la formulation de la loi, l'irrecevabilité est une hypothèse, parmi d'autres, de l'inefficacité juridique, voy. P. LECOCQ et B. VANBRABANT, *op. cit.*, pp. 109-111; L. GUINOTTE, *op. cit.*, p. 559.
28. Voy. les travaux préparatoires de la loi du 3 juin 2007 portant des dispositions diverses relatives au travail, *Doc. parl.*, Ch. repr., sess. ord. 2006-2007, n° 3067/001, pp. 23-24; CONSEIL NATIONAL DU TRAVAIL, avis n° 1586 du 19 décembre 2006 relatif au cadre juridique pour la conclusion de contrat de travail électroniques et l'utilisation de notifications électroniques en droit du travail, p. 11; H. JACQUEMIN, « La conclusion du contrat de travail par voie électronique », *Le droit du travail à l'ère du numérique*, Limal, Anthemis, 2011, pp. 33-34.

Il reste à déterminer de quelle manière les articuler, sachant que leur domaine d'application est différent. À la lumière des hypothèses dans lesquelles la loi du 9 juillet 2001, d'une part, l'article 1322, alinéa 2, du Code civil, d'autre part, doivent être observés, on pourrait penser que la première constitue la règle générale et le second la règle spéciale. La loi s'applique en effet quels que soient les objectifs poursuivis par la signature – protéger la partie faible, par exemple, ou seulement garantir la sécurité des relations contractuelles – alors que l'article 1322, alinéa 2, ne vise que la signature requise en matière probatoire – autrement dit, pour garantir la sécurité des relations contractuelles. Ces dispositions doivent toutefois être lues en combinaison avec l'article XII.15, § 2, 2e tiret, du C.D.E., aux termes duquel « l'exigence, expresse ou tacite, d'une signature est satisfaite dans les conditions prévues soit à l'article 1322, alinéa 2, du Code civil, soit à l'article 4, § 4, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification » (clause transversale particulière). De nombreuses difficultés ont ainsi été résolues, eu égard au champ d'application, assez large, de cette dernière disposition. Cependant, il demeure des hypothèses dans lesquelles elle ne peut être invoquée (*supra*, n° 6). En outre, des discussions existent au moment de circonscrire son domaine d'application; celles-ci expliquent d'ailleurs qu'un article 3*bis*, relatif notamment à la signature du contrat de travail conclu par voie électronique, ait été introduit dans la loi du 3 juillet 1978 relative aux contrats de travail[28].

8. Règlement eIDAS. L'objet du règlement eIDAS est énoncé en son article 1er: il « a) fixe les conditions dans lesquelles un État membre reconnaît les moyens d'identification électronique des personnes physiques et morales qui relèvent d'un schéma d'identification électronique notifié d'un autre État membre; b) établit des règles applicables aux services de confiance, en particulier pour les transactions électroniques; et c) instaure un cadre juridique pour les services de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de documents électroniques, d'envoi recommandé électronique et les services de certificats pour l'authentification de site internet ».

Le champ d'application des dispositions du règlement doit être circonscrit à la lumière des notions utilisées, telles que définies à l'article 3,

tout en tenant compte des limites posées à l'article 2. En particulier, le règlement ne « s'applique pas à la fourniture de services de confiance utilisés exclusivement dans des systèmes fermés résultant du droit national ou d'accords au sein d'un ensemble défini de participants »[29].

S'agissant spécialement des services de confiance, le règlement ne limite pas son application aux hypothèses dans lesquelles les formalités seraient requises dans une perspective probatoire ou pour d'autres finalités, telles les exigences requises *ad validitatem* (étant entendu, par ailleurs, qu'il « n'affecte pas le droit national ou de l'Union relatif à la conclusion et à la validité des contrats ou d'autres obligations juridiques ou procédurales d'ordre formel » (art. 2, § 3)). Peu importe également que les services de confiance soient utilisés dans le secteur privé ou dans le secteur public, de manière transfrontalière ou purement nationale[30].

Deux précisions doivent être ajoutées concernant l'application du règlement eIDAS.

Sous réserve des dispositions listées à l'article 52, § 2, le règlement est applicable à partir du 1er juillet 2016. Des mesures transitoires sont établies à l'article 51, relativement aux certificats et dispositifs de signature électronique qui auraient été établis conformément à la directive 1999/93/CE (ou les lois de transposition)[31].

Ensuite, il faut souligner que le règlement ne fixe pas la totalité du cadre normatif en matière d'identification électronique[32] ou de services de confiance. Il laisse ainsi une certaine marge de manœuvre aux législateurs des États membres. Tel est le cas pour les services de confiance qu'il ne vise pas expressément (typiquement, l'archivage électronique)[33]. Il en

29. Le considérant n° 21 du règlement donne l'exemple des « systèmes institués par des entreprises ou des administrations publiques pour gérer les procédures internes et utilisant des services de confiance ne devraient pas être soumis aux exigences du présent règlement », tout en précisant que « seuls les services de confiance fournis au public ayant des effets sur les tiers devraient remplir les exigences du présent règlement ».
30. Pour l'identification électronique, le règlement va moins loin puisqu'il se focalise sur les hypothèses d'e-gouvernement (le secteur privé étant par ailleurs encouragé à utiliser les moyens d'identification, sur une base volontaire – *cf.* le considérant n° 17) et l'utilisation des moyens d'identification électronique dans une perspective transfrontalière. Pour une comparaison entre les dispositions du chapitre II et du chapitre III du règlement, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : évolution ou révolution », *op. cit.*, pp. 31 et s.
31. Pour davantage de détails sur ce point, voy. D. GOBERT, « Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS) : évolution ou révolution », *op. cit.*, pp. 49-50.
32. S'agissant de l'identification électronique, les États membres restent en effet libres de mettre en place des schémas d'identification électronique et, ensuite, de les notifier conformément à la procédure établie par le règlement. Celui-ci ne s'applique en effet qu'aux schémas qui ont été notifiés (art. 2, § 1er, du règlement).
33. Voy. le considérant n° 25 du règlement eIDAS.

va de même des aspects qui ne sont pas harmonisés par le règlement (par exemple, les effets juridiques des services de confiance, qui ne bénéficient pas de l'assimilation ou de la présomption établie par le règlement)[34]. On doit normalement s'attendre à ce que, d'ici le 1er juillet 2016, le législateur belge amende le cadre normatif en vigueur, pour supprimer les dispositions légales ou réglementaires applicables aux questions désormais harmonisées par le règlement, tout en complétant, le cas échéant, les domaines dans lesquels il retrouve sa marge de manœuvre.

Section 2

Enjeux de la réglementation et principes directeurs

9. Pourquoi et comment réguler la matière ? Pour comprendre précisément les raisons de l'intervention du législateur, en droit de l'Union ou en droit national, pour lever les obstacles formels à la conclusion des contrats en ligne ou encadrer les activités de certains prestataires de services de confiance, il faut revenir brièvement sur les principales questions posées par la preuve (en droit privé, mais compris au sens large) dans l'environnement numérique.

C'est, en effet, pour leur apporter une réponse adéquate que le législateur a consacré plusieurs principes directeurs – parfois de manière implicite – et les a ensuite appliqués, avec plus ou moins de rigueur, aux hypothèses rencontrées.

L'analyse détaillée des dispositions de la loi du 9 juillet 2001, des articles XII.15 et XII.16 du C.D.E., ou du récent règlement eIDAS montre en effet qu'elles constituent une mise en œuvre de ces principes aux formalités rencontrées (*infra*, sect. 3).

A. *Questions posées par la preuve dans l'environnement numérique*

10. Approche finalisée. L'objectif final du législateur est de faire en sorte que les entreprises, les citoyens et les autorités publiques utilisent les technologies de l'information et de la communication dans leurs transactions électroniques, au niveau national et au niveau international. Or, ils ne le feront que s'ils ont confiance... (voy. *infra*, pt 1).

Cette confiance ne se commande pas et dépend du niveau (plus ou moins élevé) de sécurité juridique et technique qui peut leur être garanti (voy. *infra*, pt 2). Pour ce faire, il faut lever les obstacles formels à l'utili-

34. Voy. le considérant n° 22 du règlement eIDAS.

sation des technologies de l'information dans les relations contractuelles, tout en assurant l'identification des parties contractantes.

1. Garantir la confiance dans les transactions électroniques au niveau national et international

11. La confiance comme élément-clé du développement du commerce électronique. Le recours proportionné et bien pensé aux technologies de l'information et de la communication dans les transactions électroniques constitue assurément un facteur de croissance et de développement économique. Encore faut-il que toutes les parties prenantes – entreprises, citoyens et autorités publiques – aient suffisamment confiance pour y recourir[35].

Relevons quelques éléments susceptibles de compromettre cette confiance.

Les fraudes ou, plus largement, la cybercriminalité, sont indéniablement présentes dans l'environnement numérique: contrairement aux relations contractuelles nouées dans un environnement traditionnel, les parties n'ont pas nécessairement l'occasion de se rencontrer et d'être en présence physique l'une de l'autre. Aussi peut-on craindre des usurpations d'identité ou des tentatives de *phishing*.

Parallèlement, dans une optique de transaction totalement dématérialisée, il n'est plus possible de signer à la main le contrat papier, d'y apposer la mention requise légalement, et d'en conserver un exemplaire original dans ses archives « physiques ». On peut alors se demander si le document électronique muni d'une signature digitale et archivé dans le *cloud* aura la même valeur juridique (et les mêmes effets, sur le plan probatoire, notamment), que le document papier correspondant.

À l'aune de ces besoins, et dans le but d'instaurer un climat de confiance, des mesures doivent être prises, pour garantir un niveau élevé de sécurité juridique et technique (*infra*, pt 2). Tel est du reste l'un des objectifs principaux du règlement eIDAS, tel qu'énoncé au considérant n° 2: « le présent règlement vise à susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur en fournissant un socle commun pour des interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques et en accroissant ainsi l'efficacité des services en ligne publics et privés, ainsi que de l'activité économique et du commerce électronique dans l'Union ». C'était également l'un des objectifs de la directive sur le commerce électronique[36], ce

35. En ce sens, voy. le considérant n° 1 et l'art. 1er du règlement eIDAS.
36. Voy. not. le considérant n° 7 de la directive sur le commerce électronique.

qui explique que le législateur français ait intitulé son texte de transposition « la loi pour la confiance dans l'économie numérique ».

12. Développement du marché intérieur. Comme toute politique défendue en droit de l'Union, il échet que les mesures adoptées contribuent au fonctionnement du marché intérieur[37].

Dans le domaine des technologies de l'information et de la communication, qui font fi des frontières physiques traditionnelles, on comprend sans peine à quel point cet enjeu est primordial. Il faut en effet permettre une fourniture transfrontalière des services en ligne, sur tout le territoire de l'Union européenne (voire au-delà, pour autant que faire se peut), de sorte qu'un prestataire belge puisse fournir des procédés de signature et de recommandé électroniques à un citoyen danois qui conclut un contrat avec une entreprise espagnole. D'un point de vue économique, l'entreprise belge passe ainsi d'un marché de 11 millions à 500 millions de clients potentiels. Elle autorise également les bénéficiaires des services – dans l'exemple, les cocontractants danois et espagnols – à jouir pleinement d'un espace sans frontières et sans obstacles à l'exercice des libertés économiques consacrées par le Traité sur le fonctionnement de l'Union européenne.

Pour atteindre cet objectif, les moyens à mettre en œuvre sont principalement d'ordre juridique et d'ordre technique.

D'un point de vue juridique, il faut s'assurer qu'il existe un socle minimal de règles harmonisées au sein des différents États membres. Si chaque État établit ses propres règles en matière de signature électronique ou de recommandé électronique, les prestataires devront modaliser leurs services au cas par cas, État par État, en fonction des bénéficiaires de ceux-ci (ou, plus vraisemblablement, renoncer à fournir ceux-ci au-delà des frontières). Dans cette matière particulièrement, les initiatives nationales manquent de sens et, à court ou moyen terme, risquent de se solder par un échec. Le législateur européen en est parfaitement conscient, raison pour laquelle il a pris, très tôt, des directives sur la signature électronique et sur le commerce électronique. Ces instruments s'étant manifestement révélés insuffisants, le règlement eIDAS a été adopté. S'agissant de la directive sur la signature électronique, le considérant n° 3 du règlement indique que celle-ci « régissait les signatures électroniques sans fournir de cadre transfrontalier et intersectoriel complet pour des transactions électroniques sécurisées, fiables et aisées à utiliser. Le présent règlement renforce et développe l'acquis que représente ladite directive ». Désormais, d'autres services de confiance (que la signature) sont visés et un niveau

37. Voy. l'art. 1er et les considérants 3-6 du règlement eIDAS.

d'harmonisation renforcé doit normalement être atteint (puisqu'il s'agit d'un règlement qui laisse moins de marge d'appréciation aux États[38]).

D'un point de vue technique également, il est indispensable que l'interopérabilité des solutions soit garantie, autrement dit que le citoyen belge puisse, par exemple, utiliser sa carte d'identité électronique pour s'authentifier auprès d'une administration publique française ou pour signer un contrat avec une entreprise suédoise (ce qui suppose que l'entreprise suédoise puisse reconnaître et valider la signature électronique du citoyen belge). Il faut donc que les technologies soient compatibles entre elles et que les systèmes puissent «se parler». Actuellement, on reste malheureusement très loin du compte, même si diverses initiatives ont été prises, en termes de normalisation, dans le domaine (on songe à la norme ISO 29115 ou aux documents produits dans le cadre du projet Stork[39]).

2. Assurer un niveau élevé de sécurité juridique et technique

13. Moyens à mettre en œuvre ? Un climat de confiance entre toutes les parties prenantes (fin) ne pourra s'établir que si un niveau élevé de sécurité juridique et technique est garanti (moyen). Dans ce cadre, plusieurs mesures peuvent être prises.

Il faut d'abord lever les obstacles formels – principaux ou accessoires – aux transactions électroniques (*infra*, n^os^ 14 et s.).

Parallèlement, l'identification des parties doit être garantie (*infra*, n° 16).

14. Lever les obstacles formels «principaux». En droit des obligations et des contrats, les exigences de forme sont légions. À la lumière de l'évolution du droit des contrats, de nombreux auteurs observent d'ailleurs une renaissance du formalisme contractuel dès le début du XX^e^ siècle[40]. Il faut toutefois attendre la seconde moitié du siècle, et spécialement la

38. On verra cependant que, dans certains domaines, la marge de manœuvre dont disposent les États reste grande (*infra*, n° 37).
39. Voy. https://www.eid-stork2.eu.
40. En ce sens, P. MOENECLAEY, *De la renaissance du formalisme dans les contrats en droit civil et commercial français*, Paris, L.G.D.J., 1914, pp. 56-57 et pp. 181-183 (à propos de la vente à tempérament, l'auteur précise que le formalisme de ce contrat, «bien que souple, n'a plus [...] pour but d'obtenir la sécurité et de faciliter les relations d'affaire mais bien plutôt d'entraver le développement et le succès de ces ventes à tempérament et surtout de protéger l'acheteur [...]»). Voy. aussi R. DEMOGUE, *Traité de droit des obligations en général. I. Les sources*, t. 1, Paris, Librairie Arthur Rousseau, 1923, pp. 315-316, qui précise que «le formalisme dans nos civilisations avancées tend à renaître [...] pour protéger certaines classes sociales (actionnaires en cas d'apport, ouvriers en cas d'accident du travail, etc.)».

dernière décennie de celui-ci[41], pour que la tendance connaisse un développement considérable, principalement en droit du travail ou en droit de la consommation[42].

Dans la présente contribution, on se limitera à un aperçu des principales formalités requises par le Code civil, à des fins probatoires (étant entendu que l'exercice peut également être fait pour les autres sortes de formalités[43]).

41. Il faut préciser que si les textes adoptés à partir des années nonante constituent la manifestation principale du phénomène de renaissance, nombre d'entre eux se substituent à d'autres législations, en vigueur depuis plusieurs décennies, et prescrivent déjà l'accomplissement de formalités diverses, quoique moins nombreuses.
42. Cet objectif est souligné par la doctrine. Voy. notamment J. FLOUR, «Quelques remarques sur l'évolution du formalisme», *Le droit privé français au milieu du XX^e^ siècle. Études offertes à Georges Ripert*, Paris, L.G.D.J., 1950, t. 1, pp. 93 et s.; J.-L. BAUDOUIN, «Rapport général», *La protection des consommateurs (Journées canadiennes)*, Travaux de l'Association Henri Capitant, t. XXIV (1973), Paris, Dalloz, 1975, pp. 8 et s.; B. BERLIOZ-HOUIN et G. BERLIOZ, «Le droit des contrats face à l'évolution économique», *Études offertes à Roger Houin*, Paris, Dalloz-Sirey, 1985, pp. 11 et s.; P. LE TOURNEAU, «Quelques aspects de l'évolution des contrats», *Mélanges offerts à Pierre Raynaud*, Paris, Dalloz-Sirey, 1985, pp. 366-367, n° 36; Ph. JESTAZ, «L'évolution du droit des contrats spéciaux dans la loi depuis 1945», *L'évolution contemporaine du droit des contrats. Journées René Savatier (Poitiers, 24-25 octobre 1985)*, Paris, P.U.F., 1986, p. 128; J. MESTRE, «L'évolution du contrat en droit privé français», *L'évolution contemporaine du droit des contrats. Journées René Savatier (Poitiers, 24-25 octobre 1985)*, Paris, P.U.F., 1986, p. 48; Th. BOURGOIGNIE, *Eléments pour une théorie du droit de la consommation au regard des développements du droit belge et du droit de la communauté économique européenne*, Bruxelles, E. Story-Scientia, 1988, pp. 211-212, n° 96; J. GHESTIN, *Traité de droit civil. La formation du contrat*, 3^e^ éd., Paris, L.G.D.J., 1993, pp. 336 et s., n^os^ 373 et s., spéc. pp. 341-342, n° 380; M. FONTAINE, «La protection de la partie faible dans les rapports contractuels (Rapport de synthèse)», *La protection de la partie faible dans les rapports contractuels. Comparaisons franco-belges* (J. GHESTIN et M. FONTAINE dir.), Paris, L.G.D.J., 1996, pp. 627-628, n° 19; F. DOMONT-NAERT, «Les relations entre professionnels et consommateurs en droit belge», *La protection de la partie faible dans les rapports contractuels. Comparaisons franco-belges* (J. GHESTIN et M. FONTAINE dir.), Paris, L.G.D.J., 1996, p. 225, n° 13; P. VAN OMMESLAGHE, «Le consumérisme et le droit des obligations conventionnelles: révolution, évolution ou *statu quo* ?», *Hommages à Jacques Heenen*, Bruxelles, Bruylant, 1994, pp. 533-537, n^os^ 13-17; X. LAGARDE, «Observations critiques sur la renaissance du formalisme», *J.C.P.*, I, 170, 1999, pp. 1767 et s., n° 40, pp. 1768-1769; G. COUTURIER, «Les finalités et les sanctions du formalisme», *Rép. Defrénois*, 2000, p. 885; M. DEMOULIN et E. MONTERO, «La conclusion des contrats par voie électronique», *Le processus de formation du contrat. Contributions comparatives et interdisciplinaires à l'harmonisation du droit européen* (M. FONTAINE dir.), Bruxelles, Bruylant, Paris, L.G.D.J., 2002, pp. 705-706, n° 18; P. WÉRY, «Le droit commun des obligations contractuelles face à l'émergence des nouvelles législations», *Le Code civil entre ius commune et droit privé européen*, Bruxelles, Bruylant, 2005, pp. 401-403, n° 8; H. JACQUEMIN, *Le formalisme contractuel. Mécanisme de protection de la partie faible*, *op. cit.*, pp. 37 et s., n° 17; P. VAN OMMESLAGHE, *Droit des obligations*, t. 1^er^, Bruxelles, Bruylant, 2010, pp. 113 et s.
43. Pour un aperçu récent, voy. H. JACQUEMIN, «Heurs et malheurs du formalisme contractuel comme mécanisme de protection du consommateur», *D.C.C.R.*, 2013/100-101, pp. 267-286.

Conformément à l'article 1341 du Code civil, l'écrit est requis en matière civile pour prouver les actes juridiques d'une valeur supérieure à 375 EUR ou pour prouver contre ou outre un écrit. Plus précisément, sauf exception, les témoignages et les présomptions sont irrecevables. Il peut s'agir d'un acte authentique ou, le plus souvent, d'un acte sous seing privé. Autrement dit, dans cette dernière hypothèse, une double formalité doit être accomplie: un écrit doit être établi et celui-ci doit être revêtu de la signature de celui qui s'oblige et contre lequel la preuve doit être apportée. Des formalités complémentaires sont prescrites par les articles 1325 et 1326 du Code civil. Le premier impose d'établir autant d'exemplaires (originaux) qu'il y a de parties ayant un intérêt distinct, tout en indiquant sur ceux-ci le nombre d'exemplaires qui ont été établis (c'est la formalité du «double» ou des «originaux multiples»). Quant à l'article 1326 du Code civil, il prescrit la formalité du «bon pour» suivant laquelle, pour les actes unilatéraux contenant une obligation de payer une somme d'argent ou une chose appréciable, le débiteur doit rédiger en entier et à la main la reconnaissance de dette ou, à tout le moins, il doit apposer la mention manuscrite «bon pour...» ou «approuvé pour...» suivie de la somme ou de la quantité de chose écrite en toutes lettres. En substance, le formalisme probatoire établi par le Code civil peut donc exiger un écrit, une signature, des exemplaires multiples et/ou des mentions manuscrites.

Avec l'avènement de la société de l'information s'est posé la question de savoir comment accomplir valablement les formes prescrites par voie électronique, dès lors qu'elles avaient généralement été conçues par référence au papier[44]. Des difficultés, d'ordre juridique[45], peuvent être

44. Au niveau européen, les États membres étaient tenus de lever les obstacles formels à la conclusion des contrats par voie électronique: voy. l'art. 9 de la directive sur le commerce électronique. Le considérant n° 34 de la directive confirme que les exigences de forme sont clairement visées. Aux termes de ce considérant, «chaque État membre doit ajuster sa législation qui contient des exigences, notamment de forme, susceptibles de gêner le recours à des contrats par voie électronique. Il convient que l'examen des législations nécessitant cet ajustement se fasse systématiquement et porte sur l'ensemble des étapes et des actes nécessaires au processus contractuel, y compris l'archivage du contrat. Il convient que le résultat de cet ajustement soit de rendre réalisables les contrats conclus par voie électronique [...]». Des obstacles étrangers aux règles de forme pourraient également être rencontrés (à ce sujet, voy. M. DEMOULIN et E. MONTERO, «Le formalisme contractuel à l'heure du commerce électronique», *op. cit.*, pp. 160-161 et les exemples cités). La délégation au Roi, prévue par l'article 16, § 3, de la LSSI et devenue caduque aujourd'hui, avait notamment pour objet de lever ces obstacles (*ibid.*, pp. 190 et s.).

45. On dénombre également des obstacles d'ordre *pratique* mais ils ne retiennent pas notre attention. En ce sens, voy. le considérant n° 37 de la directive sur la signature électronique: «l'obligation faite aux États membres d'éliminer les obstacles à l'utilisation des contrats électroniques ne concerne que les obstacles résultant d'exigences juridiques et non pas les obstacles d'ordre pratique résultant d'une impossibilité d'utiliser les moyens électroniques dans certains cas». Voy. aussi les travaux préparatoires de la LSSI, *Doc. parl.*, Ch. repr., sess. ord. 2002-2003, n° 2100/001, p. 42; M. DEMOULIN et E. MONTERO, «Le formalisme contractuel à l'heure du commerce électronique», *op. cit.*, pp. 159-160).

rencontrées[46] lorsque, pour exiger l'accomplissement d'une formalité donnée, le législateur utilise un terme désignant un procédé qui ne peut être mis en œuvre que dans l'environnement traditionnel: l'exigence d'une mention écrite de la main de celui qui s'oblige, telle que prévue par l'article 1326 du Code civil, notamment, illustre ce type de difficulté. En général, les termes utilisés ne désignent pas un procédé qui ne peut, en aucun cas, être accompli dans l'environnement numérique dans la mesure où ils pourraient être interprétés largement[47]. C'est le cas pour l'écrit, la signature ou les exemplaires multiples. Ces exigences posent toutefois un double problème au moment de les accomplir dans l'environnement numérique. D'une part, on pourrait imaginer que le juge appelé à se prononcer sur la question de savoir si les formalités ont été valablement accomplies rejette toute interprétation large de la notion d'écrit ou de signature ou, tout en acceptant une telle interprétation, décide néanmoins que le procédé mis en œuvre ne peut être qualifié de la sorte (parce qu'il ne posséderait pas certaines qualités)[48]. D'autre part, le risque existe également que le juge accepte de qualifier d'écrit ou de signature des

46. À ce sujet, voy. les travaux préparatoires, qui distinguent les obstacles directs et indirects. Ils énoncent que «les obstacles directs résultent, par exemple, de l'exigence formelle d'un prospectus papier ou d'une écriture à la main. Les obstacles indirects résultent plutôt des exigences de forme, qui ne spécifient pas expressément le type de support mais qui créent une insécurité juridique dans la mesure où il n'est pas certain qu'elles puissent être appliquées au contrat électronique (les notions de formulaire, avenant, bon de commande, etc.)» (*Doc. parl.*, Ch. repr., sess. ord. 2002-2003, n° 50-2100/001, p. 42). Voy. aussi M. DEMOULIN et E. MONTERO, «Le formalisme contractuel à l'heure du commerce électronique», *op. cit.*, pp. 157 et s.

47. La formalité de l'«écrit» (ou ses succédanés fonctionnels), de la «signature» ou des «exemplaires multiples» renvoie, il est vrai, à un procédé déterminé dans l'environnement traditionnel (un support papier recouvert de signes exprimant un langage pour l'écrit; un graphisme personnel tracé directement sur le support, pour la signature; l'établissement de plusieurs supports dont le contenu est identique et qui sont revêtus de la signature de celui qui s'oblige, pour les exemplaires multiples). À la faveur d'une interprétation large, on pourrait toutefois estimer qu'un procédé électronique, accompli dans l'environnement numérique, puisse être qualifié de la sorte, sans forcément méconnaître la définition du terme. On observe en effet qu'à l'origine, lorsque s'est posée la question de savoir comment accomplir les formes en recourant aux technologies de l'information, les auteurs ont défini les concepts traditionnels par référence, notamment, à leurs fonctions, de sorte que les procédés accomplis dans l'environnement numérique puissent être visés (voy. not. M. FONTAINE, «La preuve des actes juridiques et les techniques nouvelles», *op. cit.*, pp. 6-9; J. LARRIEU, *op. cit.*, pp. 11 et s., n^{os} 13 et s.). Pourquoi, en effet, ne pas considérer qu'un fichier *Word* est un écrit, qu'un mécanisme de cryptographie asymétrique est une signature et que ce fichier *Word*, associé à un mécanisme de cryptographie asymétrique et transmis par courrier électronique à chacun des cocontractants répond à l'exigence des exemplaires multiples?

48. Dans ces hypothèses, le recours aux technologies de l'information pour nouer les rapports contractuels soumis aux législations retenues serait gravement compromis: les prestataires pourraient en effet hésiter à profiter des opportunités offertes par l'internet, par crainte de voir leurs conventions contestées ou annulées.

procédés qui ne permettent pas d'atteindre les fonctions généralement reconnues aux procédés mis en œuvre pour accomplir ces formalités dans l'environnement papier[49].

Globalement, ces deux problèmes trouvent leur source dans l'insécurité juridique tenant à la manière d'accomplir valablement les formes requises dans l'environnement numérique.

Nous verrons que, pour y répondre, le législateur a consacré la théorie des équivalents fonctionnels (*infra*, n° 21). Les autres principes directeurs – principes de non-discrimination et d'assimilation et principe de neutralité technologique – participent du même objectif (*infra*, n^{os} 18 et s.).

En droit belge, on trouve des réponses à ces difficultés à l'article XII.15 du Code de droit économique, qui consacre la théorie des équivalents fonctionnels et l'applique aux principales formalités (l'écrit, la signature et la mention manuscrite). S'agissant de la signature, il faut aussi se référer à l'article 1322, alinéa 2, du Code civil et à la loi du 9 juillet 2001 sur la signature électronique et les P.S.C. À divers égard, ces règles devront être amendées pour tenir compte des modifications introduites par le règlement eIDAS en matière de signature électronique, de cachet électronique et, dans une moindre mesure, de document électronique. On note d'ailleurs que, pour la signature et le cachet, l'intervention d'un prestataire de service de confiance s'impose.

15. Lever les obstacles formels «accessoires». Au-delà des difficultés liées à l'accomplissement, en tant que tel, des principales formalités requises dans l'environnement numérique (écrit, signature et formalités complémentaires aux mentions), la question s'est aussi posée de savoir comment accomplir valablement d'autres exigences, accessoires à celles-ci.

Elles sont principalement de trois ordres et présentent un grand intérêt pratique, notamment en matière probatoire.

Elles peuvent d'abord avoir pour objet de déterminer précisément *le moment* auquel une formalité a été accomplie (et, par voie de conséquence, à quel moment est intervenu l'acte juridique ainsi constaté). Il n'est en effet pas rare que des délais très stricts doivent être observés pour poser un acte (exercer son droit de rétractation en matière de contrat à distance ou notifier la résiliation d'un contrat, par exemple)[50]. C'est aussi sur la base de cette information que l'on déterminera par exemple si les parties avaient la capacité de contracter ou quelle était la loi applicable.

49. Dans ce cas, les formes imposées par le législateur pour protéger l'un des cocontractants, jugé en position de faiblesse, et dont la multiplication est incontestable, perdraient tout leur sens.

50. Pour un panorama des exigences en la matière, voy. M. DEMOULIN, «Aspects juridiques de l'horodatage des documents électroniques», *Commerce électronique: de la théorie à la pratique*, Cahier du CRID, n° 23, Bruxelles, Bruylant, 2003, pp. 48 et s.

L'article 1328 du Code civil peut certes être invoqué mais, en pratique, les hypothèses limitativement énumérées sont rarement rencontrées. Dans l'environnement numérique, on aura recours à des procédés d'horodatage électronique.

Les formalités accessoires peuvent aussi avoir trait à la *transmission* de l'information (constatée dans un écrit signé, par exemple). On veut dans ce cas s'assurer que l'information a été envoyée et/ou reçue par son destinataire. Dans l'environnement traditionnel, on peut faire appel à un huissier ou s'adresser à *bpost* pour envoyer un courrier recommandé. Dans l'environnement numérique, c'est le service de recommandé électronique qui devrait jouer ce rôle.

Enfin, il ne suffit pas d'avoir accompli valablement une formalité dans l'environnement traditionnel ou numérique. Encore faut-il *conserver* le document, et être ainsi en mesure de le produire ultérieurement, en cas de litige avec un cocontractant, ou au moment de démontrer aux autorités publiques que les exigences prescrites légalement ont été observées. La durée de conservation variera en fonction de l'hypothèse considérée étant entendu qu'à défaut de règles spécifiques, on aura généralement égard au délai de prescription de droit commun, soit dix ans (art. 2262*bis* C. civ.). Le recours aux technologies de l'information permet de révolutionner les politiques d'archivages traditionnelles consistant à classer les documents «papier» dans d'interminables rayonnages de caisses et de classeurs. En recourant à l'archivage électronique, il est non seulement possible de conserver dans un environnement dématérialisé des documents établis au format électronique, mais également de numériser des documents «papier», de manière à les conserver uniquement au format électronique (et détruire ultérieurement le document originaire «papier»).

Dans chacune de ces hypothèses, des enjeux similaires doivent être pris en considération. À quelles conditions peut-on juger que le service d'horodatage, de recommandé ou d'archivage électronique apporte des garanties suffisantes pour fixer précisément le moment auquel la formalité a été accomplie ou pour être équivalent à un service de recommandé papier, opéré par exemple par *bpost*, ou à une politique d'archivage classique ? Dans tous les cas, l'intervention d'un prestataire de confiance, opérant le service d'horodatage, de recommandé ou d'archivage, est requis.

Des initiatives ont été prises au niveau belge pour encadrer certains de ces services mais, pour la plupart, elles n'ont pas abouti (sur ce point, voy. *supra*, n° 5). Aussi faut-il principalement avoir égard au règlement eIDAS, qui encadre certains de ces services de confiance (horodatage électronique, recommandé électronique et authentification de site internet). Mis à part une disposition ponctuelle[51], ce règlement ne contient pas de

51. Voy. l'art. 34 du règlement.

règles en matière d'archivage électronique (aussi ne l'examinerons-nous pas dans la présente contribution[52]). On espère donc que les propositions avancées au niveau belge sur ce thème renaissent de leurs cendres.

16. Identifier ou authentifier l'identité. La confiance entre les parties à une transaction électronique ne peut s'instaurer que si elles ont des garanties leur permettant d'identifier leur correspondant ou, en tout cas, d'authentifier son identité avec un niveau de certitude plus ou moins grand. En effet, dans l'environnement numérique, les parties ne sont pas en présence physique l'une de l'autre, ce qui empêche d'identifier son cocontractant *de visu*, en se référant, le cas échéant, à un document d'identité officiel (tel une carte d'identité ou un passeport); en outre, il n'est guère très compliqué de créer une adresse de courrier électronique au nom d'un tiers ou un faux site internet. Cela vaut principalement pour les personnes physiques, même si on peut étendre le raisonnement aux personnes morales.

Le besoin existe dans les relations avec les autorités publiques (pour bénéficier des services d'e-gouvernement) et dans le secteur privé.

Concrètement, des outils existent déjà en Belgique. On pense à la carte d'identité électronique qui offre une double fonction d'authentification et de signature électronique. Divers mécanismes présentant un niveau élevé de sécurité juridique ont aussi été implémentés dans le secteur bancaire (spécialement pour accéder aux services d'internet ou de mobile banking). On aura d'ailleurs noté le lien étroit entre cette exigence d'identification (ou d'authentification de l'identité) et la formalité de la signature.

Les principales difficultés ont trait aux garanties offertes par ce moyen d'identification (ou d'authentification) et à la possibilité de l'utiliser pour des services transfrontiers en ligne.

Le législateur y répond dans le règlement eIDAS, en consacrant un important chapitre à l'identification électronique. Seule l'utilisation de ces moyens dans une relation transfrontalière nouée avec une autorité publique est toutefois concernée. S'agissant d'une question qui n'est pas en lien direct avec la preuve en droit privé, nous ne l'examinons pas dans la présente contribution[53].

52. À ce sujet, voy. M. DEMOULIN (dir.), *L'archivage électronique et le droit*, Collection du CRIDS, Bruxelles, Larcier, 2012.
53. Voy. D. GOBERT, «Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS): évolution ou révolution», *op. cit.*, pp. 33 et s.

B. *Principes directeurs*

17. Consécration, expresse ou implicite, de plusieurs principes directeurs. Pour lever les obstacles formels principaux et accessoires, plusieurs principes directeurs ont été consacrés et sont mis en œuvre, avec plus ou moins de bonheur, par le législateur européen et le législateur belge.

Nous nous penchons successivement sur le principe de non-discrimination (qui reçoit une double portée), sur le principe d'équivalence fonctionnelle et sur le principe de neutralité technologique.

18. Principe de non-discrimination. Conformément l'article 9, § 1er, de la directive sur le commerce électronique, «les États membres veillent à ce que leur système juridique rende possible la conclusion des contrats par voie électronique. Les États membres veillent notamment à ce que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ni ne conduise à priver d'effet et de validité juridiques de tels contrats pour le motif qu'ils sont passés par voie électronique».

Ponctuellement, pour certaines formalités particulières, on constate que le législateur a confirmé expressément sa position, en énonçant que la formalité requise ne pouvait pas être privée d'effets juridiques ou, à tout le moins, être dépourvue de certains de ces effets, sous prétexte qu'elle avait été accomplie par voie électronique. Ainsi, l'article 4, § 5, de la loi du 9 juillet 2001 sur la signature électronique et les P.S.C. stipule qu'«une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif [...] que la signature se présente sous forme électronique [...]»[54]. Cette disposition consacre le principe de non-discrimination, auquel est généralement associé le principe d'assimilation[55].

Comme on le verra, avec le règlement eIDAS, le principe de non-discrimination est appliqué aux services de confiance (exception faite, logiquement, de l'authentification de site internet) et au document électronique, en interdisant que l'effet juridique ou la recevabilité comme preuve en justice leur soient refusés au seul motif qu'ils se présentent sous forme électronique (*infra*, nos 24 et 36).

54. On note que cette disposition transpose littéralement l'article 5, § 2, de la directive sur la signature électronique.
55. Sur ces deux principes, voy. not. E. MONTERO, «Définition et effets juridiques de la signature électronique en droit belge: appréciation critique», *D.A.O.R.*, 2002, pp. 13 et s.; D. GOBERT et E. MONTERO, «L'ouverture de la preuve littérale aux écrits sous forme électronique», *J.T.*, 2001, pp. 116-117; P. LECOCQ et B. VANBRABANT, «La preuve du contrat conclu par voie électronique», *Le commerce électronique: un nouveau mode de contracter*, Liège, Éd. du Jeune Barreau, 2001, pp. 106 et s.; M. ANTOINE et D. GOBERT, «La directive européenne sur la signature électronique. Vers la sécurisation des transactions sur l'Internet?», *J.T.D.E.*, 2000, pp. 74-75, nos 5-8.

Le principe doit être bien compris: interdire qu'une formalité soit privée d'effet juridique au seul motif qu'elle est accomplie par voie électronique ne signifie pas qu'elle est, *ipso facto*, jugée équivalente au procédé correspondant dans l'environnement papier (avec les mêmes effets juridique). Pour tirer cette conclusion, il faut démontrer que les fonctions de la formalité, telles qu'énoncées par le législateur ont été atteintes (le cas échéant, en se basant sur une clause d'assimilation ou une présomption établie légalement, comme le fait le règlement eIDAS avec les services de confiance qualifiés).

Ce raisonnement en deux temps (non-discrimination *certaine* dans un premier temps avec, dans un second temps, la *possible* reconnaissance d'une équivalence avec le procédé traditionnel ou du respect des fonctions attendues du procédé) n'est pas sans poser de question.

L'affirmation du principe de non-discrimination peut se comprendre si l'on envisage la formalité – par exemple la signature – dans une perspective probatoire. On sait en effet que la méconnaissance des règles de preuve se traduit, sur le terrain de la sanction, en termes de recevabilité et de valeur (ou de force) probante. On peut concevoir qu'un moyen de preuve soit recevable (principe de non-discrimination) mais ne possède pas de force probante (inapplication en l'espèce de l'équivalence). Par contre, s'agissant des formalités qui ne sont pas requises (uniquement) dans une perspective probatoire, il n'y a pas de sanction intermédiaire. Par exemple, en l'absence de signature valable, l'acte juridique est nul ou converti. Le principe de non-discrimination n'a pas vraiment d'intérêt: ce qui importe, c'est de savoir si la signature électronique est assimilée à une signature manuscrite. À défaut, la sanction doit en principe être appliquée.

En somme, ces dispositions ont une vertu pédagogique, en ce qu'elles réaffirment le principe suivant lequel le recours aux technologies de l'information ne doit pas empêcher l'accomplissement des formalités qu'elles concernent. Rien n'empêche dès lors de les maintenir, même si l'adoption de dispositions spécifiques, indiquant comment accomplir les formes par voie électronique, implique nécessairement que la formalité peut être observée dans l'environnement numérique.

On verra que le régime du règlement en matière de services de confiance est construit sur une distinction fondamentale entre (prestataire de) service de confiance qualifié et (prestataire de) service de confiance non-qualifié (*infra*, nos 30 et s.). Pour souligner la liberté des parties de recourir à l'un ou à l'autre, une déclinaison du principe de non-discrimination leur est appliquée, de sorte que l'effet juridique ou la recevabilité comme preuve en justice d'un service de confiance ne peut leur être refusée au seul motif qu'il ne satisfait pas aux conditions du service de confiance qualifié[56].

56. Art. 25, § 1er, 35, § 1er, 41, § 1er, et 43, § 1er, du règlement eIDAS.

19. Principe d'équivalence fonctionnelle. Dans le courant des années quatre-vingt, parallèlement aux progrès techniques, des auteurs ont rapidement cerné les enjeux juridiques posés par le développement de l'informatique et des technologies de l'information. Ils ont esquissé les premières solutions en la matière, essentiellement sous l'angle du droit de la preuve[57]. Si d'autres solutions ont également été proposées[58], la théorie des équivalents fonctionnels a progressivement pris corps, avant d'être consacrée, au niveau international, par la CNUDCI, dans sa loi-type sur le commerce électronique[59] (1996). Les travaux de celle-ci ont inspiré le législateur européen et le législateur belge.

Ce principe part du constat que les procédés mis en œuvre dans l'environnement papier pour accomplir les formes prescrites ne peuvent être reproduits comme tels lorsque le contrat est conclu par voie électronique. Si l'on souhaite que des rapports contractuels puissent être noués par ce biais, il doit être possible d'identifier les procédés à mettre en œuvre dans l'environnement numérique. Suivant la théorie des équivalents fonction-

57. Voy. en ce sens les réflexions de B. AMORY et Y. POULLET, «Le droit de la preuve face à l'informatique et à la télématique: approche de droit comparé», *D.I.T.*, 1985/5, pp. 11 et s.; M. FONTAINE, *op. cit.*, pp. 1 et s.; J. LARRIEU, *op. cit.*, pp. 8 et s.; N. VERHEYDEN-JEANMART, *op. cit.*, pp. 233-234, nos 492-493; Y. POULLET, «Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve», *Le droit des affaires en évolution. Le juriste face à l'invasion informatique*, Bruxelles, Bruylant, 1996, pp. 39 et s.; E. DAVIO, «Preuve et certification sur Internet», *R.D.C.*, 1997, pp. 660 et s.; R. STEENNOT, «Juridische problemen in het kader van de elektronische handel», *R.D.C.*, 1999, pp. 671 et s.

58. Plusieurs alternatives ont été proposées en doctrine pour résoudre les difficultés posées par l'accomplissement des formes dans l'environnement numérique. Sur ces arguments, voy. B. AMORY et Y. POULLET, *op. cit.*, pp. 16-17; M. FONTAINE, *op. cit.*, pp. 16-20; J. LARRIEU, *op. cit.*, pp. 8-9; Fr. LABARTHE, *La notion de document contractuel*, Paris, L.G.D.J., 1994, pp. 73 et s., nos 95 et s.; Y. POULLET, *op. cit.*, pp. 42-44, n° 5; R. STEENNOT, *op. cit.*, pp. 672-673; D. GOBERT et E. MONTERO, «La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle», *D.A.O.R.*, 2000, p. 18. Voy. aussi l'exposé des motifs du projet de loi visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations, *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, n° 2141/001, pp. 13-15.

59. Comme indiqué dans le Guide pour son incorporation, «la Loi type propose [...] une nouvelle approche, parfois désignée sous l'appellation 'approche fondée sur l'équivalent fonctionnel', qui repose sur une analyse des objectifs et des fonctions de l'exigence traditionnelle de documents papier et vise à déterminer comment ces objectifs ou fonctions pourraient être assurés au moyen des techniques du commerce électronique» (*Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation*, New-York, Publ. des Nations Unies, 1999, p. 21, n° 16). À ce propos, voy. de E. CAPRIOLI et R. SORIEUL, «Le commerce international électronique: vers l'émergence de règles juridiques transnationales», *J.D.I.*, 2, 1997, p. 382: «Dans leur tentative d'apporter une solution juridique à certains obstacles rencontrés par le commerce électronique, les auteurs de la loi-type se sont constamment référés aux situations juridiques connues dans le monde des documents-papier pour imaginer comment de telles situations pourraient être transposées, reproduites ou imitées dans un environnement dématérialisé». Voy. aussi l'excellente analyse de M. DEMOULIN, *Droit du commerce électronique et équivalents fonctionnels*, Bruxelles, Larcier, 2014.

nels, on ne définit pas une exigence de forme par référence à un procédé technique particulier (le support papier pour l'écrit, le graphisme personnel et manuscrit apposé directement sur le support pour la signature, etc.) mais à la lumière des fonctions qu'elle permet de remplir (garantir la lisibilité, la pérennité, voire l'intégrité de l'information, pour l'écrit, par exemple). Deux procédés accomplis respectivement dans l'environnement traditionnel (le support papier pour l'écrit, par exemple) et dans l'environnement numérique (un document au format pdf enregistré sur un CD-ROM pour l'écrit, par exemple) sont alors jugés *équivalents* s'ils permettent de remplir les *fonctions* minimales reconnues à la formalité (l'écrit, en l'occurrence). Cette équivalence entre les procédés signifie que, sur le plan juridique, ils ont les mêmes effets et sont interchangeables. Autrement dit, la formalité prescrite est valablement accomplie dans l'environnement numérique lorsque le procédé choisi permet d'atteindre les fonctions reconnues à l'exigence.

En droit belge, ce principe est consacrée à l'article XII.15, § 1er, du Code de droit économique, aux termes duquel «toute exigence légale ou réglementaire de forme relative au processus contractuel est réputée satisfaite à l'égard d'un contrat par voie électronique lorsque les qualités fonctionnelles de cette exigence sont préservées». Le paragraphe 2 de cette disposition applique ensuite la théorie aux formalités rencontrées le plus souvent en pratique: l'écrit, la signature et la mention manuscrite.

Dans certains cas, il n'est toutefois pas nécessaire à l'interprète de la norme de se fonder sur cette théorie puisque le recours possible aux technologies de l'information est directement pris en considération par le législateur, qui désigne les formalités à accomplir au moyen de termes neutres (obligation d'accuser réception ou de transmettre des informations) ou spécialement adaptés soit à l'environnement traditionnel (le support papier), soit à l'environnement numérique (le support durable).

Sans l'affirmer expressément, le règlement eIDAS semble appliquer le principe d'équivalence fonctionnelle aux formalités qu'il vise puisque, comme on le verra, les procédés susceptibles d'être utilisés sont définis par référence aux fonctions attendues d'eux. Ces fonctions sont déterminées à l'aune du procédé correspondant dans l'environnement papier, en tout cas lorsqu'il existe, même s'il faut constater qu'à divers égards, l'équivalence fonctionnelle est loin d'être parfaite.

20. Principe de neutralité technologique. Le principe *de neutralité technologique* est à la base de toutes les interventions normatives en lien avec l'accomplissement des formes dans l'environnement numérique[60]. Suivant celui-ci, les dispositions normatives doivent rester neutres et ne

60. Voy. le considérant n° 8 de la directive sur la signature électronique ou la loi type de la CNUDCI de 2001 sur les signatures électroniques et le Guide pour son incorporation,

pas désigner expressément une technologie déterminée: eu égard à la rapidité des progrès scientifiques et techniques, il est en effet hautement probable que cette technologie devienne à brève échéance totalement obsolète. Il faudrait dès lors modifier les textes normatifs continuellement, pour qu'ils correspondent aux standards techniques minimaux, de nature à maintenir le niveau de sécurité requis.

Dans certains cas, on peut douter qu'il ait été parfaitement observé. La méthode choisie par le législateur dans la loi sur le contrat de travail (art. 3*bis*) et consistant à désigner un procédé particulier – en l'espèce la signature électronique créée par la carte d'identité électronique – est contestable dans la mesure où elle méconnaît ce principe[61].

Section 3

Analyse systématique des mesures prises pour lever les obstacles formels dans le domaine probatoire

A. *Les obstacles formels levés sans l'intervention d'un service de confiance*

21. Principe d'équivalence fonctionnelle consacré de manière générale et appliqué à l'écrit et aux mentions manuscrites. Certains obstacles à l'accomplissement des formes dans l'environnement numérique peuvent être levés sans que l'intervention d'un prestataire de service de confiance soit absolument nécessaire.

C'est notamment le cas pour l'écrit, la mention manuscrite ou l'établissement d'exemplaires multiples.

Pour ces exigences, il convient en effet d'appliquer les clauses transversales particulières (art. XII.15, § 2: pour l'écrit et la mention manuscrite) ou la clause transversale générale (art. XII.15, § 1er: pour les exemplaires multiples).

En pratique, des prestataires de confiance pourraient toutefois prendre part au processus de dématérialisation, compte tenu des formalités complémentaires à respecter par ailleurs (signature, archivage, horodatage, etc.). Il est en effet assez rare que l'exigence de l'écrit ne doive pas être complétée par une signature, et ne fasse ensuite l'objet de mesure de conservations.

New York, Publ. des Nations Unies, 2002, p. 35, n° 82. Voy. aussi, plus récemment les considérants nos 26 et 27 du règlement eIDAS.

61. À ce propos, voy. H. JACQUEMIN, «La conclusion du contrat de travail par voie électronique», *Le droit du travail à l'ère du numérique* (K. ROSIER dir.), Limal, Anthemis, 2011, pp. 15 et s.

22. Écrit ou support durable. Les fonctions attendues de l'écrit sont énoncées à l'article XII.15, § 2, du C.D.E., aux termes duquel «l'exigence d'un écrit est satisfaite par une suite de signes intelligibles et accessibles pour être consultés ultérieurement, quels que soient leur support et leurs modalités de transmission». Le procédé utilisé dans l'environnement numérique doit ainsi garantir la lisibilité, la pérennité et, même si cette fonction est plus controversée, l'intégrité de l'information[62].

Les dispositions légales les plus récentes utilisent le terme «support durable». La notion est notamment définie dans le C.D.E., qui comprend la notion comme «tout instrument permettant au consommateur ou à l'entreprise de stocker des informations qui lui sont adressées personnellement d'une manière permettant de s'y reporter ultérieurement pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées»[63]. Il ressort de cette définition que le support durable doit remplir trois fonctions[64] (lisibilité, pérennité, et même si cette fonction est plus discutée, intégrité de l'information), à l'instar de l'écrit (ou du papier dans l'environnement traditionnel). Il constitue donc un équivalent fonctionnel de l'écrit[65]. Comme l'a indiqué la Cour de Justice de l'Union européenne dans l'arrêt *Content Services*[66], à propos de l'alternative entre l'écrit et le support durable, «le législateur de l'Union a prévu deux solutions fonctionnellement équivalentes et, ainsi, une exigence d'équivalence de tels supports. Dans ces conditions [...], un substitut au support papier peut être considéré comme étant susceptible de correspondre aux exigences de protection du consommateur dans le contexte des nouvelles technologies à condition qu'il remplisse les mêmes fonctions que le support papier» (pts 40 et 41 de l'arrêt).

62. Sur les fonctions de l'écrit, voy. H. JACQUEMIN, *Le formalisme contractuel. Mécanisme de protection de la partie faible, op. cit.*, pp. 121 et s., n^os^ 73 et s. (avec les réf. citées).
63. Art. I.8, 19°, du C.D.E.
64. Voy. H. JACQUEMIN, *Le formalisme contractuel. Mécanisme de protection de la partie faible, op. cit.*, pp. 367 et s., n° 278. Reprenant également ces trois fonctions, voy. M. DEMOULIN, «La notion de 'support durable' dans les contrats à distance: une contrefaçon de l'écrit?», *R.E.D.C.*, 2000, p. 364.
65. Voy. M. DEMOULIN, «La notion de 'support durable' dans les contrats à distance: une contrefaçon de l'écrit?», *op. cit.*, p. 375, qui note qu'«à bien y regarder, on relève de troublantes similitudes entre la mystérieuse notion de support durable... et celle d'écrit. Par un heureux hasard, les fonctions que chacun serait amené à remplir sont identiques et, d'ailleurs, par un heureux hasard, tout aussi controversées». L'auteur aborde alors le caractère controversé de la fonction d'inaltérabilité.
66. C.J.U.E., 5 juillet 2012, aff. C-49/11, *Content Services Ltd.* Pour un commentaire de cet arrêt, voy. H. JACQUEMIN, «Arrêt '*Content Services*': l'exigence du support durable dans les contrats à distance», *J.D.E.*, 2012, pp. 243-246; S. DE POURCQ, «De informatieverplichting bij verkoop op afstand: een hyperlink die naar een gewone website leidt, volstaat niet», note sous C.J.U.E., 5 juillet 2012, *D.C.C.R.*, 2012/4, pp. 57 et s.

Le considérant n° 23 de la directive sur les droits des consommateurs[67] donne des exemples de procédés susceptibles d'être qualifiés de supports durables (ou, par voie de conséquence, d'écrit, puisqu'il s'agit d'équivalents fonctionnels). Sont ainsi mentionnés «le papier, les clés USB, les CD-Rom, les DVD, les cartes à mémoire ou les disques dur d'ordinateur ainsi que les courriels». Plus discutée est la question de savoir si une page web répond, ou pas, à la définition fonctionnelle du support durable. Certaines pages web sont modifiées à un rythme quasi ininterrompu, par une multitude d'intervenants (l'intégrité des informations n'est, par conséquent, pas garantie). Dans l'arrêt *Content Services*, la C.J.U.E. a ainsi jugé qu'«il ne ressort pas du dossier que le site Internet du vendeur auquel renvoie le lien indiqué au consommateur permet à ce dernier de stocker des informations qui lui sont personnellement adressées de manière telle qu'il puisse y accéder et les reproduire telles quelles pendant une durée appropriée en dehors de toute possibilité de modification unilatérale de leur contenu par le vendeur» (point 46).

23. Mention manuscrite. En ce qui concerne la mention manuscrite (requise, par exemple, à l'article 1326 du Code civil), on peut se référer à l'article XII.15, § 2, 3^e^ tiret, du C.D.E., aux termes duquel «l'exigence d'une mention écrite à la main de celui qui s'oblige peut être satisfaite par tout procédé garantissant que la mention émane bien de ce dernier». Le verbe «émaner» met l'accent sur l'origine de la mention. Le procédé doit garantir que le débiteur, et lui seul, est l'auteur de la mention.

Deux conditions, cumulatives, doivent être satisfaites.

Il faut *d'abord* que la mention soit rédigée par celui qui s'oblige. Une intervention active de sa part est requise. Concrètement, la partie faible peut être invitée à dactylographier le texte, au moyen du clavier de son ordinateur, dans une zone déterminée, sur une page du site web du prestataire. Aussi longtemps que le texte de la mention ne correspond pas exactement à celui prescrit par la loi, le processus de conclusion du contrat ne peut se poursuivre. Il est insuffisant qu'elle se borne à cocher une case à côté de laquelle figure le texte en question, préalablement rédigé par son cocontractant. Dans cette hypothèse, en effet, c'est ce dernier qui est à l'origine de la mention (c'est de lui qu'elle *émane*) et pas le débiteur. Peu importe si, par ailleurs, ce dernier procédé permet en principe d'établir que le débiteur a pris connaissance du contenu de la mention.

Ensuite, il faut nécessairement garantir que l'auteur de la mention est effectivement le débiteur, et pas son cocontractant (ou un tiers). C'est

67. Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil, *J.O.*, L 304 du 22 novembre 2011.

la fonction d'authentification de l'origine. Dans l'environnement traditionnel, la personnalisation du graphisme remplit cette fonction. En général, cette caractéristique n'existe pas dans l'environnement numérique: le recours au clavier de l'ordinateur conduit en effet à uniformiser le graphisme. Un procédé complémentaire doit être mis en œuvre. Un mécanisme de signature électronique pourrait convenir. Le débiteur devrait activer son logiciel de signature électronique, lorsqu'il introduit la mention requise dans la zone prédéfinie. Il ne nous paraît pas suffisant de subordonner l'accès à la partie transactionnelle du site à l'introduction d'un login et d'un mot de passe. Ce procédé permet de garantir – avec une efficacité relative mais suffisante – que l'auteur de la mention est celui qu'il prétend être et pas un tiers. Cependant, en l'occurrence, le danger ne vient pas d'un tiers mais du cocontractant de la partie faible. Or, en tant que titulaire du site, il peut *a priori* accéder au login et au mot de passe de l'autre partie. Cette technique ne l'empêche donc nullement d'introduire lui-même la mention prescrite par la loi.

24. Principe de non-discrimination applicable au document électronique. Le document électronique est défini de manière large par le règlement eIDAS comme «tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel»[68]. La notion est plus large que l'écrit puisque le contenu peut également être sonore, visuel ou audiovisuel. Par contre, aucune indication n'est donnée relativement aux fonctions attendues de la formalité.

Le règlement eIDAS applique le principe de non-discrimination au document électronique, en énonçant que «l'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique» (art. 46).

La proposition de la Commission du 4 juin 2012 était nettement plus ambitieuse puisqu'elle indiquait les fonctions à respecter pour que le document électronique soit jugé équivalent au document imprimé.

On peut se demander comment articuler cette disposition avec la clause transversale particulière relative à l'écrit (figurant à l'art. XII.15, § 2, du C.D.E.). Lorsque l'hypothèse entre dans le champ d'application de l'article 46 du règlement (clause de non-discrimination pour le document électronique) et de l'article XII.15, § 2, du C.D.E. (fonctions à respecter pour que le procédé soit jugé équivalent à l'écrit), aucune difficulté ne se pose. La clause de non-discrimination est d'ailleurs implicitement visée à l'article XII.15, § 2, du C.D.E. Par contre, si la formalité constitue un document électronique soumis à la clause de non-discrimination de l'article 46 du règlement mais échappe au domaine d'application de l'article XII.15,

68. Art. 3, 35°, du règlement.

§ 2, du C.D.E. (parce qu'il ne s'agit pas d'un «écrit» ou que l'hypothèse est expressément exclue par l'article XII.16 du C.D.E.), des discussions sont permises. Conformément au principe de non-discrimination, le juge ne peut pas écarter le procédé. Il n'est toutefois pas tenu, nécessairement, de le juger équivalent au procédé «papier» correspondant. La difficulté tient toutefois au fait qu'il ne peut pas se fonder sur l'article XII.15, § 2, du C.D.E., et les conditions établies par celui-ci. À défaut de disposition légale réglant expressément la question en droit interne, il incomberait à la personne qui entend se prévaloir du procédé à des fins probatoires de démontrer que les fonctions traditionnellement reconnues à la formalité ont été préservées (tout en suggérant d'appliquer, par analogie, les conditions de l'article XII.15, § 2, du C.D.E.).

B. *Les obstacles formels levés par l'intervention d'un service de confiance*

1. Panorama des services de confiance visés par le règlement eIDAS

25. Services de confiance et règlement eIDAS. Au sens du règlement eIDAS, le prestataire de confiance est «une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié»[69].

Quant au service de confiance, il désigne «un service électronique normalement fourni contre rémunération qui consiste:

a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services; ou

b) en la création, en la vérification et en la validation de certificats pour l'authentification de site internet; ou

c) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services»[70].

26. Signature électronique et cachet électronique. La signature électronique s'entend «des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer»[71]. Le règlement eIDAS introduit la notion de cachet électronique, qu'il définit comme «des données sous

69. Art. 3, 19°, du règlement.
70. Art. 3, 16°, du règlement.
71. Art. 3, 10°, du règlement.

forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières »[72].

On verra que les régimes respectifs de la signature électronique et du cachet électronique sont très proches l'un de l'autre (*infra*, nos 35 et s.). Aussi examinons-nous les notions en parallèle.

Plusieurs éléments distinguent cependant les deux procédés. Le signataire[73] est une personne physique. Le créateur du cachet est une personne morale. Les fonctions attendues du procédé mis en œuvre diffèrent également. La signature électronique est utilisée pour signer. Le règlement eIDAS n'en dit toutefois pas davantage, et ne détaille pas les effets juridiques de la signature[74]. En droit privé belge, on admet généralement que les fonctions traditionnellement attendues de la signature manuscrite consistent à marquer l'adhésion du signataire au contenu de l'acte et à authentifier son identité[75]. D'après le règlement eIDAS, le cachet ne poursuit pas les mêmes fonctions que la signature puisqu'il vise uniquement à garantir l'origine et l'intégrité des données[76]. Il peut par exemple être utilisé pour démontrer qu'un document électronique – ou un bien numérique, tel un logiciel – a été établi par une personne morale et n'a

72. Art. 3, 25°, du règlement.
73. Autrement dit, la « personne physique qui crée une signature électronique » (art. 3, 9°, du règlement).
74. Voy. à ce sujet l'art. 2, § 3, du règlement.
75. Voy. H. JACQUEMIN, *Le formalisme contractuel. Mécanisme de protection de la partie faible*, *op. cit.*, pp. 99 et s., nos 59 et s. Cette dernière fonction est, du reste, la plus importante. À nos yeux, la fonction d'authentification est secondaire par rapport à celle-ci. L'authentification de l'origine n'est pas une fin en soi. On comprendrait d'ailleurs difficilement qu'il en soit autrement, eu égard à l'efficacité, assez réduite, du mécanisme: il n'est guère impossible de reproduire une signature manuscrite (en utilisant un calque, par exemple). En outre, la signature ne crée qu'une présomption réfragable, suivant laquelle elle émane de la personne qui s'en prétend l'auteur, et qu'il est possible de renverser. La fonction d'authentification ne doit être vue que comme une condition d'efficacité de la fonction d'adhésion: il s'agit d'un moyen entièrement dédié à la mise en œuvre de cette autre fonction. En effet, la signature ne peut manifester la volonté de son auteur de s'approprier le contenu de l'acte si ce n'est pas lui, mais un tiers, qui a accompli la formalité.
76. Il ne s'agit donc pas de la signature électronique d'une personne morale. On note que la loi du 9 juillet 2001 consacre expressément la signature électronique des personnes morales, en son article 4, § 4. L'assimilation automatique des signatures électroniques avancées qui respectent les conditions établies par cette disposition s'applique en effet sans préjudice « qu'elle soit réalisée par une personne physique ou *morale* » (nous soulignons). Concrètement, la signature ne serait plus celle de la personne physique, intervenant au titre d'organe de la société, pour engager celle-ci, mais celle de la personne morale (même si, *de facto*, une personne physique devra *a priori* intervenir pour activer le logiciel de signature). Sur la signature électronique des personnes morales, voy. B. VANBRABANT, « La signature électronique des personnes morales », *La preuve*, Liège, Formation permanente CUP, 2002, pp. 174 et s. Voy. aussi *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, no 322/001, pp. 15 et s.

pas subi de modification[77]. Rien n'empêche cependant que le législateur belge utilise la marge de manœuvre laissée par le règlement en vue de donner au cachet des effets juridiques similaires à ceux de la signature.

Qu'il s'agisse de la signature ou du cachet électronique, le règlement introduit trois types de procédés: la signature – ou le cachet – électronique (simple)[78], la signature – ou le cachet – électronique avancé(e)[79] et la signature – ou le cachet électronique – qualifié(e)[80]. Chaque procédé est une déclinaison du précédent, soumis à des conditions complémentaires (et bénéficiant d'un régime spécifique). On se réjouit que le législateur européen ait expressément consacré la notion de signature électronique « qualifiée », déjà utilisé par la doctrine[81] et, de manière ponctuelle, par le législateur belge[82].

Par contre, on regrette que le règlement ait maintenu un régime aussi complexe, qui exige d'articuler trois définitions et donc, trois procédés de signature ou de cachet électronique. Pour la signature, il faut au moins ajouter un quatrième procédé dont les conditions sont établies à l'article 1322, alinéa 2, du Code civil. Cette manière de faire est d'autant plus contestable qu'à l'analyse, les effets juridiques de certains procédés sont assez réduits (*infra*, no 37).

77. Voy. les considérants nos 59 et 65 du règlement eIDAS.
78. Ceux-ci répondent aux définitions référencées *supra*, aux notes 72 et 73.
79. La signature électronique avancée est « la signature électronique qui satisfait aux exigences énoncées à l'article 26 » (art. 3, 11°, du règlement eIDAS). Plus précisément, cette disposition exige que la signature satisfasse aux exigences suivantes: « a) être liée au signataire de manière univoque »; b) « permettre d'identifier le signataire; c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif; et d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable ». Ces conditions renforcent les fonctions d'identification, d'authentification et de maintien de l'intégrité du contenu de l'acte. Suivant le même modèle, le cachet électronique est « un cachet électronique qui satisfait aux exigences énoncée à l'article 36 » (art. 3, 26°, du règlement), cette disposition énonçant les mêmes conditions que celles figurant à l'article 26 pour la signature électronique avancée.
80. La signature électronique qualifiée est « une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique » (art. 3, 12°, du règlement). Les notions de « dispositif de création de signature électronique qualifié » et de certificat qualifié de signature électronique » sont définies par le règlement (art. 3, 15° et 23°). Le même modèle est suivi pour le cachet électronique qualifié (art. 3, 27°, pour la définition et art. 3, 30° et 32° pour les notions auxquelles celle-ci fait référence).
81. E. MONTERO, « Définition et effets juridiques de la signature électronique en droit belge: appréciation critique », *D.A.O.R.*, 2002/61-62, p. 14, no 6, note 10.
82. Voy. l'art. 2, 3°, de la loi du 10 juillet 2006 relative à la procédure par voie électronique, *M.B.*, 7 septembre 2006 ou l'art. 1er, 4°, de l'arrêté du Gouvernement wallon du 12 juin 2014 portant exécution du décret du 27 mars 2014 relatif aux communications par voie électronique entre les usagers et les autorités publiques wallonnes, *M.B.*, 1er octobre 2014.

2

On peut également se demander si les principes d'équivalence fonctionnelle et de neutralité technologique, qui auraient normalement dû présider à la rédaction de ces clauses, ont été préservés.

Il est d'abord heureux que, par rapport à la définition de la signature électronique (simple) ou qualifiée figurant dans la directive de 1999 (et la loi du 9 juillet 2001), la fonction de « signer » ait été expressément ajoutée. L'examen des conditions posées à l'article 4, § 4, de la loi du 9 juillet 2001 pour que la signature électronique qualifiée soit assimilée à une signature manuscrite montre, en effet, qu'il n'est pas expressément requis que le procédé permette de marquer l'adhésion de son auteur au contenu de l'acte[83]. En négligeant de souligner cette importante fonction de la signature, le législateur omet de prendre en considération une différence majeure entre la signature manuscrite et le procédé de signature électronique. La fonction d'adhésion de la signature manuscrite résulte en effet de la portée symbolique que le geste revêt dans l'environnement traditionnel : en signant, on prend conscience qu'un engagement est pris et que désormais, il ne pourra en principe être délié unilatéralement sans motif et sans pénalités. Pour l'heure, le procédé de signature électronique n'emporte pas de telles conséquences. En activant le logiciel de signature électronique, l'internaute peut ne pas avoir conscience de son engagement. Le règlement eIDAS corrige cette lacune puisque l'acte de « signer », en droit privé des obligations, signifie que le scripteur marque son adhésion au contenu. On note d'ailleurs que, si l'article 1322, alinéa 2, du Code civil n'énonce pas expressément la fonction de l'adhésion au contenu de l'acte, à la lecture des travaux préparatoires, il semble que l'on puisse la déduire de la notion d'imputabilité[84].

83. La solution est également critiquable à la lumière du considérant 20 de la directive sur la signature électronique, aux termes duquel « les signatures électroniques avancées qui sont basées sur des certificats qualifiés et qui sont créées par un dispositif sécurisé de création de signature ne peuvent être considérées comme étant équivalentes, sur le plan juridique, à des signatures manuscrites que si les exigences appliquées aux signatures manuscrites ont été respectées ». Tel n'est pas le cas en l'espèce. L'origine de la lacune réside dans le texte même de la directive, que le législateur belge a transposé littéralement. Pourtant, la première version de la proposition de directive y faisait référence (proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, *J.O.C.E.*, C 325 du 23 octobre 1998, p. 1).

84. Voy. à ce propos E. MONTERO, « Introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique 'fonctionnaliste' ? », *Mélanges offerts à Marcel Fontaine*, Bruxelles, Larcier, 2003, p. 191, n° 9-2 : « on ne saurait donc estimer que l'imputabilité de la signature implique en tout état de cause l'adhésion au contenu. En revanche, la signature reconnue ou non contestée crée une présomption *juris et de jure* que le signataire a donné son consentement au contenu de l'acte. En principe, on considérera que l'*animus signandi* se manifeste, par exemple, lors de la saisie, par le signataire, du code secret permettant l'activation de sa clé cryptographique. Néanmoins, il n'est pas exclu qu'un juge estime, en cas de contestation, que telle signature électronique, bien qu'imputable à telle personne, n'atteste pas son intention de s'approprier le contenu de l'acte. Même si cette condition n'est pas inscrite explicitement

Par contre, comme sous l'empire de la directive de 1999 et des dispositions de transposition (l'article 4, § 4, de la loi du 9 juillet 2001 ou l'article 1322, alinéa 2, du Code civil)[85], le règlement eIDAS exige de la signature électronique qu'elle préserve davantage de fonctions que la signature manuscrite.

S'agissant de l'authentification de l'origine, la signature électronique qualifiée offre des garanties que la signature manuscrite classique est loin d'apporter. À nos yeux, cette différence ne doit toutefois pas être critiquée. En effet, il ne s'agit pas de la seule catégorie de signature électronique susceptible d'être jugée équivalente, sur le plan des effets, à une signature manuscrite. Le cas échéant, on peut se fonder sur l'article 1322, alinéa 2, du Code civil. Et il paraît raisonnable que le législateur soit plus exigeant dans la mesure où, conformément à l'article 4, § 4, de la loi du 9 juillet 2001 ou l'article 25, § 2, du règlement eIDAS, l'assimilation est automatique (le juge ne disposant normalement d'aucun pouvoir d'appréciation).

On peut par contre regretter que la signature électronique qualifiée, la signature électronique avancée et celle régie par l'article 1322, alinéa 2, du Code civil ajoutent une fonction que la signature manuscrite ne permet pas de remplir : la fonction d'intégrité[86]. Comment expliquer que le législateur ait ajouté cette exigence ? Dans l'environnement traditionnel, l'intégrité du contenu est principalement garantie par le support papier. Dans l'environnement numérique, le support papier n'existe plus. Or, le procédé technique généralement présenté comme garantissant les fonctions de la signature électronique – la cryptographie asymétrique – permet effectivement de préserver l'intégrité des informations. Le législateur a donc exigé de la signature électronique qu'elle remplisse cette fonction. Sur le plan des principes, cette solution ne se justifie pas. Il eût été plus cohérent, selon nous, que cette fonction d'intégrité soit exigée de l'écrit[87]. En définitive, nous plaidons pour que le législateur belge amende

dans le texte, elle y figure implicitement sous la notion d'imputabilité éclairée par les travaux préparatoires, et se déduit, du reste, de la théorie générale de la signature ».

85. À ce propos, voy. H. JACQUEMIN, *Le formalisme contractuel. Mécanisme de protection de la partie faible*, *op. cit.*, pp. 410 et s., n° 304.

86. Pour un regard critique sur la fonction d'intégrité, requise par l'art. 1322, al. 2, C. civ., voy. E. MONTERO, « Définition et effets juridiques de la signature électronique en droit belge : appréciation critique », *op. cit.*, pp. 24-25 ; D. MOUGENOT, *La preuve*, *op. cit.*, p. 194, n° 122-3.

87. En outre, conformément au principe de l'équivalence fonctionnelle, il n'est pas nécessaire de trouver un procédé et un seul, qui remplirait toutes les fonctions de l'écrit ou toutes les fonctions de la signature, dans l'environnement numérique. On peut mettre en œuvre une combinaison de procédés. En pratique, rien n'empêche que la fonction d'intégrité de l'écrit soit remplie par une signature électronique. On pourrait aussi imaginer que la signature électronique ne permette pas de préserver l'intégrité du contenu mais que celle-ci soit garantie au moyen du procédé mis en œuvre au titre de l'écrit (en confiant le document à un prestataire d'archivage, par exemple). En

l'article 1322, alinéa 2, du Code civil, de manière à supprimer l'exigence d'intégrité du contenu. Ce faisant, il ménagerait le principe d'équivalence fonctionnelle et simplifierait les obligations des parties qui souhaiteraient utiliser un mécanisme de signature électronique (d'autant qu'à l'analyse, mais de manière critiquable, la jurisprudence belge néglige de vérifier si la fonction a effectivement été préservée[88]).

27. Horodatage électronique. On entend par horodatage électronique « des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant »[89].

Le mécanisme est intéressant dans la mesure où il ne connaît pas, en tant que tel, d'équivalent dans l'environnement « papier ». On peut soit se fonder sur l'une des hypothèses visées à l'article 1328 du Code civil, qui donnent date certaine aux actes sous seing privé, soit établir un acte authentique. À défaut, la date de l'envoi recommandé à la poste peut être invoquée mais elle constitue tout au plus une présomption de l'homme.

Deux fonctions sont ainsi requises du procédé d'horodatage électronique : indiquer la date et l'heure avec précision et garantir l'intégrité des données auxquelles se rapportent cette date et cette heure[90].

l'occurrence, cette solution ne peut toutefois être admise *de lege lata*. Il est vrai que, dans la plupart des cas, cette caractéristique critiquable de la signature électronique aura une incidence limitée dans la mesure où l'écrit et la signature sont généralement exigés conjointement. Telle est probablement la raison pour laquelle un auteur estime qu'« il eût mieux valu poser le maintien de l'intégrité comme une condition de l'acte sous seing privé électronique, sans exiger que cette intégrité résulte du mécanisme de signature. Il importe peu, en définitive, que l'intégrité de l'acte invoqué en justice soit fonction de l'écriture, du support ou de la signature. Dès lors que l'intégrité de l'acte est attestée et que le mécanisme de signature utilisé par les parties permet de les identifier et d'exprimer leur adhésion, faut-il dénier à ce dernier la qualité de signature au motif qu'il n'établit pas, par lui-même, le maintien de l'intégrité du contenu de l'acte ? » (E. MONTERO, « Introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique "fonctionnaliste' ? », *op. cit.*, p. 192, n° 10). En définitive, la fonction d'intégrité doit donc être garantie, peu importe qu'on l'attribue à l'écrit ou à la signature. Globalement, toutes les fonctions de l'écrit et de la signature seront préservées. Dans certains cas, cependant, l'écrit ne doit pas nécessairement être signé.

88. Voy. C. trav. Bruxelles, 11 octobre 2013 et 14 février 2014, *R.D.T.I.*, 2014/56, p. 115 et la note de J.-B. HUBIN, « Signature scannée : quand une technologie simple confronte le juriste à des questions complexes ». Dans l'arrêt du 11 octobre 2013, la Cour du travail avait bien noté l'exigence du maintien de l'intégrité. Pourtant, dans l'arrêt du 14 février 2014 (la Cour ayant posé des questions aux parties et ordonné une réouverture des débats), elle accorde des effets juridiques à une signature scannée sans vérifier que la fonction a effectivement été préservée.
89. Art. 3, 33°, du règlement.
90. Voy. l'art. 41, § 2, du règlement, qui énonce clairement ces fonctions et présume qu'elles sont remplies dans l'hypothèse de l'horodatage électronique qualifié.

Une distinction est faite également entre l'horodatage électronique (simple) et l'horodatage électronique qualifié, qui doit satisfaire aux conditions de l'article 42[91].

Ce dernier doit apporter des garanties complémentaires en lien avec les deux fonctions précitées. L'article 42, § 1er, du règlement exige ainsi que soient satisfaites les exigences suivantes : « a) il lie la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données ; b) il est fondé sur une horloge exacte liée au temps universel coordonné ; et c) il est signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente ».

28. Service d'envoi recommandé électronique. Le service d'envoi recommandé électronique est le « service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée »[92].

Le règlement eIDAS liste ainsi les fonctions attendues du service d'envoi recommandé électronique : preuve de l'envoi et de la réception des données et maintien de leur intégrité (puisqu'elles doivent être protégées des risques de perte, de vol ou de modification).

L'envoi recommandé est déjà défini à l'article 131, 9°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques[93] comme « un service garantissant forfaitairement contre les risques de perte, vol ou détérioration et fournissant à l'expéditeur, le cas échéant à sa demande, une preuve de la date du dépôt de l'envoi postal et/ou de sa remise au destinataire ».

Nonobstant son importance pratique considérable, l'incertitude restait de mise quant à la valeur légale des procédés de recommandé électronique. Conformément à l'article 135, § 2, de la loi du 21 mars 1991, « toutes les obligations reprises dans la présente loi et dans toutes les autres lois relatives aux matières visées à l'article 78 de la Constitution et leurs arrêtés d'exécution qui, concernant les envois recommandés, contiennent les mots "à la poste", "par la poste" ou toute autre référence du même type sont remplies lorsqu'est utilisé un envoi recommandé tel que défini à l'article 131, 9° de la présente loi ou un envoi recommandé électronique conformément à la loi du 9 juillet 2001 fixant certaines règles relatives au

91. Art. 3, 34°, du règlement.
92. Art. 3, 36°, du règlement.
93. *M.B.*, 27 mars 1991.

cadre juridique pour les signatures électroniques, le recommandé électronique et les services de certification». Le renvoi à la loi du 9 juillet 2001 est cependant erroné, toute référence au recommandé ayant été supprimée[94]. Aussi fallait-il espérer que le législateur remette l'ouvrage sur le métier pour enfin régler cette question et garantir la sécurité juridique.

C'est chose faite avec le règlement eIDAS même si on regrette que les fonctions attendues du recommandé électronique ne correspondent pas parfaitement à celles du recommandé papier traditionnel et sont en réalité plus nombreuses[95].

Comme pour les précédents services de confiance, le législateur définit le service d'envoi recommandé électronique qualifié[96] et renvoie, à ce propos, aux exigences établies à l'article 44 du règlement, qui renforce les conditions à respecter.

29. Certificat d'authentification de site internet. Le dernier service de confiance régi par le règlement eIDAS, quoique de manière partielle (voy. *infra*, nos 36 et 37), est la délivrance de certificats d'authentification de site internet. Il s'agit de l'«attestation qui permet d'authentifier un site internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré»[97]. L'objectif est clairement de lutter contre le *phishing* ou d'autres pratiques frauduleuses semblables.

Le règlement définit également le certificat qualifié d'authentification de site internet, qui doit être délivré par un prestataire de services de confiance qualifié et satisfaire aux conditions listées dans l'annexe IV.

94. La loi du 13 décembre 2010 modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges et modifiant la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (*M.B.*, 31 décembre 2010) encadrait les services de recommandé électronique et déterminait les conditions dans lesquelles le procédé mis en place pouvait être jugé équivalent au procédé traditionnel de la lettre recommandée, en introduisant diverses dispositions dans la loi sur les signatures électronique et les services de certification. Cette loi du 13 décembre 2010 a cependant été abrogée avec effet immédiat par une loi du 31 mai 2011 portant des dispositions diverses en matière de télécommunication (*M.B.*, 21 juin 2011).
95. Sur les fonctions du recommandé, voy. E. MONTERO, «Du recommandé traditionnel au recommandé électronique: vers une sécurité et une force probante renforcées», *Commerce électronique: de la théorie à la pratique*, Cahier du CRID n° 23, Bruxelles, Bruylant, 2003, pp. 75 et s. Comp. D. GOBERT, «Le règlement européen du 23 juillet 2014 sur l'identification électronique et les services de confiance (eIDAS): évolution ou révolution», *op. cit.*, pp. 47-48, qui appuie cette solution.
96. Art. 3, 37°, du règlement.
97. Art. 3, 38°, du règlement.

2. *Summa divisio* entre les (prestataires de) services qualifiés et les (prestataires de) services non-qualifiés

30. Être ou ne pas être qualifié? Le règlement établit une *summa divisio* entre, d'une part, les prestataires de services de confiance (P.S.C.) qualifiés et les services de confiance (S.C.) qualifiés, d'autre part, les prestataires de service de confiance non qualifiés et les services de confiance non qualifiés.

Les notions de «prestataire de service de confiance» et de «service de confiance» ont déjà été présentées (*supra*, n° 25). Le prestataire de service de confiance qualifié est «un prestataire de service de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut de qualifié»[98]. Le «service de confiance qualifié» est également défini par le règlement, mais de manière curieuse et, en tout état de cause, peu utile dans une perspective de qualification: il s'agit en effet du «service de confiance qui satisfait aux exigences du présent règlement»[99].

Comme on le verra, des conditions particulièrement rigoureuses doivent être observées par les prestataires s'ils veulent obtenir le statut de qualifié et lancer leur activité (*infra*, n° 33). Parallèlement, dans l'exercice même de leur activité, de nombreuses obligations leur sont imposées, en lien avec les services de confiance qu'ils délivrent (*infra*, n° 34). Il en résulte des contraintes techniques et organisationnelles importantes ainsi qu'une charge administrative et financière très lourde. Autrement dit, il est hautement probable qu'au sein des États membres, voire au niveau de l'Union, de tels prestataires soient finalement peu nombreux.

Le respect de ces conditions donne lieu à l'application d'un régime juridique plus favorable aux parties utilisatrices du service de confiance: les effets juridiques des services de confiance qualifiés leur permettent de bénéficier d'une clause d'assimilation ou d'une présomption légale (*infra*, n° 37); le prestataire qualifié est présumé avoir agi intentionnellement ou par négligence (*infra*, n° 38); les services qualifiés sont reconnus en tant que tels dans tous les États membres (*infra*, n° 39). Sur ce point, l'objectif du règlement est clair: aux termes du considérant n° 28, «pour accroître, en particulier, la confiance des petites et moyennes entreprises (P.M.E.) et des consommateurs dans le marché intérieur et pour promouvoir l'utilisation des services et produits de confiance, les notions de service de confiance qualifié et de prestataire de services de confiance qualifié devraient être introduites en vue de définir les exigences et obligations qui assurent un niveau élevé de sécurité de tous les services et produits de confiance qualifiés qui sont utilisés ou fournis».

98. Art. 3, 20°, du règlement.
99. Art. 3, 17°, du règlement.

Au contraire, les services de confiance non-qualifiés bénéficient d'effets juridiques soumis à l'aléa de la preuve (et aucune présomption ne peut être invoquée en termes de responsabilité). Le risque existe donc que la preuve ne puisse pas être apportée (même si, très clairement, et suivant le procédé utilisé, il peut fort bien ne pas se réaliser).

Tout dépend en définitive du risque que l'on est prêt à assumer, lorsque l'on recourt à un service de signature, de cachet, de recommandé ou d'horodatage électronique. Si l'enjeu financier – ou le risque en général – est faible, sans doute n'est-il pas requis de déployer l'artillerie lourde en surprotégeant l'opération: pour donner un exemple concret, on ne passe pas devant le notaire pour constater l'achat de quelques meubles de jardin entre particuliers (même si, sur le plan probatoire, la sécurité juridique est renforcée en recourant à l'acte authentique plutôt qu'à l'acte sous seing privé). Par contre, s'il s'agit d'un contrat portant sur plusieurs millions d'euros et que la date de signature est primordiale, on sera bien avisé de recourir à un service d'horodatage et de signature électroniques qualifiés (ou au service du notaire, dans l'environnement traditionnel).

31. Organe de contrôle. Pour s'assurer que les prestataires de services de confiance – spécialement les P.S.C. qualifiés – sont dignes... de la confiance que le règlement leur accorde, celui-ci impose la désignation d'un «organe de contrôle» par les États membres[100]. Son rôle est précisé par l'article 17 du règlement.

Parmi d'autres, ils sont tenus de réaliser des contrôles *a priori* et *a posteriori* des P.S.C. qualifiés (et des S.C. qualifiés qu'ils fournissent). Si nécessaire, ils doivent également prendre des mesures de contrôle *a posteriori* à l'égard des P.S.C. non qualifiés (et des S.C. qu'ils fournissent), s'ils sont informés que les dispositions du règlement seraient méconnues[101].

Le règlement pose aussi les bases d'une assistance mutuelle entre les organes de contrôle des États membres[102].

32. Exigences applicables à tous les P.S.C., qualifiés ou non-qualifiés. Le règlement eIDAS impose diverses obligations à tous les prestataires de services de confiance, qu'ils soient qualifiés ou non qualifiés.

100. L'art. 17, § 1er, du règlement exige en effet qu'ils désignent «un organe de contrôle établi sur leur territoire ou, d'un commun accord avec un autre État membre, un organe de contrôle établi dans cet autre État membre. Cet organe est chargé des tâches de contrôle dans l'État membre qui a procédé à la désignation.
Les organes de contrôle sont investis des pouvoirs nécessaires et dotés des ressources adéquates pour l'exercice de leurs tâches».
101. Sur ce point, voy. aussi le considérant n° 36 du règlement.
102. Art. 18 du règlement.

Outre le rappel général des exigences relatives à la protection de la vie privée et au traitement des données à caractère personnel[103] ainsi qu'en matière d'accessibilité aux personnes handicapées[104], les principales conditions ressortissent sans surprise au domaine de la sécurité.

L'article 19, § 1er, du règlement les oblige ainsi à prendre «les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents».

En cas d'atteinte à la sécurité ou de perte d'intégrité ayant une incidence importante sur le service fourni ou sur les données à caractère personnel qui y sont conservées, une obligation de notification pèse sur les prestataires, vis-à-vis de l'organe de contrôle[105] et, le cas échéant, des bénéficiaires des services de confiance concernés[106], conformément à l'article 19, § 2, du règlement. La notification doit intervenir dans les meilleurs délais. Pour la notification à l'organe de contrôle, le règlement impose un délai de 24 heures prenant cours à partir de leur connaissance par le prestataire de confiance. On ne négligera pas la charge (administrative et financière) que représente une telle obligation, particulièrement si le prestataire a plusieurs milliers (ou millions, pour des multinationales du secteur des télécoms, par exemple) de clients. Le cas échéant, il peut être requis d'informer les organes de contrôles d'autres États membres et l'ENISA, voire le public en général, si l'organe de contrôle décide qu'il est dans l'intérêt public de procéder à une telle divulgation[107].

33. Conditions pour lancer un service de confiance qualifié. Lorsqu'un prestataire de services de confiance veut fournir des S.C. qualifiés et obtenir le statut de P.S.C. qualifié, il doit préalablement obtenir une auto-

103. Art. 5 du règlement. Voy. aussi l'art. 24, § 2, j), uniquement applicable aux prestataires de services de confiance qualifiés, et qui leur impose d'assurer le traitement licite des données à caractère personnel conformément à la directive 95/46/CE. Voy. aussi, à ce propos, le considérant n° 11 du règlement. Sur ce thème, on note que le considérant n° 31 encourage la coopération et l'échange d'informations entre l'organe de contrôle et les autorités en charge de la protection des données.
104. Art. 15 du règlement. Voy. aussi le considérant n° 29.
105. Il peut aussi s'agir d'autres organes compétents (le règlement cite l'organisme national compétent en matière de sécurité de l'information ou l'autorité chargée de la protection des données, autrement dit la Commission de protection de la vie privée, pour la Belgique).
106. Cette exigence ne s'impose que «lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de porter préjudice à une personne physique ou morale à laquelle le service de confiance a été fourni».
107. Art. 19, § 2, du règlement.

risation de l'organe de contrôle. La procédure est décrite à l'article 21 du règlement. Le régime est ainsi diamétralement opposé à celui qui prévalait sous l'empire de la directive de 1999 en matière de signature électronique puisqu'elle interdisait aux États membres de soumettre les prestataires de services de certification à un régime d'autorisation préalable[108]. Le système mis en place par le règlement offre davantage de garanties quant au prestataire même si on peut craindre que cette exigence ait un effet dissuasif. Conformément aux lois de transpositions de la directive de 1999, les prestataires fournissant des services de signature électronique qualifiée étaient très rares. *A fortiori*, avec cette exigence additionnelle, on peut sérieusement douter qu'ils soient plus nombreux...

La notification soumise par le prestataire à l'organe de contrôle doit être accompagnée d'un rapport délivré par un organisme d'évaluation de la conformité[109].

C'est principalement sur cette base que l'organe de contrôle vérifiera le respect des exigences du règlement et, en cas d'appréciation positive, leur accordera le statut de « qualifié » (normalement dans un délai de trois mois à compter de la notification[110]).

Il est primordial que toutes parties prenantes (les parties utilisatrices, les prestataires et les autorités publiques compétentes) sachent avec certitude qui sont les prestataires qualifiés. Aussi incombe-t-il aux États membres d'établir, de publier et de mettre à jour des listes de confiance[111]. De son côté, la Commission met à la disposition du public les informations permettant de consulter ces listes (et de connaître l'organisme chargé de les publier). Cette publication sur une liste de confiance est importante puisque les prestataires ne peuvent fournir des services dits « qualifiés » qu'à partir du moment où leur statut est indiqué sur celles-ci[112]. À cet instant, ils peuvent également utiliser le label de confiance de l'Union[113] et l'apposer, par exemple, sur leur site internet ou tout autre document promotionnel.

34. Exigences applicables aux P.S.C. qualifiés (dans l'exercice de leur activité). L'article 24 du règlement liste les nombreuses exigences applicables, de manière générale, aux P.S.C. qualifiés.

108. Art. 3, § 1er, de la directive 1999/93/CE. Un régime volontaire d'accréditation pouvait toutefois être organisé (art. 3, § 2, de la directive).
109. La notion est définie l'art. 3, 18°, du règlement.
110. Le règlement autorise toutefois l'organe de contrôle à prolonger le délai pour autant qu'il informe le prestataire, en lui indiquant les raisons du retard et le délai nécessaire pour achever la mission.
111. Art. 22 du règlement.
112. Art. 21, § 3, du règlement.
113. Art. 23 du règlement.

Les prestataires qui délivrent des certificats qualifiés doivent vérifier l'identité et, éventuellement, les attributs de la personne physique ou morale à laquelle celui-ci est délivré[114]. Des règles encadrent également l'établissement et la mise à jour d'une base de données relative aux certificats, ainsi que la révocation éventuelle de ceux-ci (l'opération de révocation en tant que telle et l'information qui doit en être donnée).

Le règlement énumère aussi, au § 2 de l'article 24, diverses obligations tenant aux obligations d'information vis-à-vis de l'organe de contrôle (a) ou des parties utilisatrices (d), aux compétences de leur personnel et sous-traitants éventuels (b), aux ressources financières et aux assurances (c), à la fiabilité et à la sécurité des systèmes et produits mis en place (d à g), à l'archivage des informations pertinentes concernant les données délivrées et reçues (h), ou à la continuité de leurs activités, par la mise en place d'un plan actualisé d'arrêt (i).

En complément de ces exigences d'ordre général, il faut ajouter les conditions propres à certains services de confiance qualifiés. En matière de signature (et de cachet), le règlement détermine les exigences relatives aux certificats qualifiés de signature (ou de cachet) électronique[115], aux dispositifs de création de signature électronique qualifiés (les exigences applicables à ceux-ci, la certification des dispositifs et la publication de ceux-ci)[116], ainsi qu'à la validation et la conservation des signatures (et des cachets) électroniques qualifiés[117]. Des conditions figurent également aux annexes I à III du règlement. Pour les autres services de confiance, le règlement n'établit pas de règles additionnelles à celles qui ont déjà été abordées (*supra*, nos 32 et s.).

Le règlement impose aux P.S.C. qualifiés de faire l'objet d'un audit dont les résultats doivent être transmis à l'organe de contrôle[118]. Il doit être réalisé tous les 24 mois, aux frais du prestataire, par un organisme d'évaluation de conformité. Cet audit peut aussi être demandé par l'organisme de contrôle à tout moment[119]. L'organe de contrôle peut être amené à imposer au prestataire de corriger certains manquements aux exigences prévues par le règlement et, à défaut de réponse satisfaisante, la sanction peut aller jusqu'à priver le prestataire ou le service concerné du statut de « qualifié »[120].

114. Art. 24, § 1er, du règlement. Cette disposition indique par qui et comment cette vérification peut être faite, conformément au droit national.
115. Art. 28 pour la signature et art. 38 pour le cachet.
116. Art. 29-31 pour la signature et art. 39 pour le cachet.
117. Art. 32-34 pour la signature et art. 40 pour le cachet.
118. Art. 20, § 1er, du règlement.
119. Art. 20, § 2, du règlement.
120. Art. 20, § 3, du règlement.

Les stipulations figurant dans le règlement formulent les exigences en termes de mesures à prendre et de fonctions à préserver. Le texte ne dit donc pas, par exemple, qu'il faut respecter la norme ISO unetelle ou recourir à la cryptographie asymétrique. Compétence est toutefois donnée à la Commission européenne d'établir, au moyen d'actes d'exécution, les numéros de référence de normes (techniques ou organisationnelles) à respecter[121]. Le règlement préserve ainsi le principe de neutralité technologique, tout en permettant au secteur de disposer d'informations claires quant aux exigences techniques auxquelles les prestataires sont soumis (et que la Commission veillera à actualiser si nécessaire). Le règlement prévoit d'ailleurs que le prestataire est présumé respecter les exigences que ses dispositions énoncent lorsque les normes en question sont respectées.

3. Effets juridiques des services de confiance qualifiés ou non qualifiés

35. Des effets dépendant de la qualification ou de la non-qualification. Le règlement soumet les P.S.C. et les S.C. qualifiés à des conditions différentes des P.S.C. et des S.C. non qualifiés.

Le principe de non-discrimination s'applique à tous les services de confiance (*infra*, n° 36).

Par contre, on observe des différences importantes – et logiques – entre les effets attachés aux services de confiance qualifiés ou non qualifiés, en termes de clause d'assimilation ou de présomption (*infra*, n° 37), de responsabilité (*infra*, n° 38) et de reconnaissance internationale (*infra*, n° 39).

36. Principe de non-discrimination. Le règlement consacre expressément le principe de non-discrimination à la signature électronique[122], au cachet électronique[123], à l'horodatage électronique[124] et au service d'envoi recommandé électronique[125] (sur ce principe, voy. *supra*, n° 18).

121. Voy. les art. 24, § 5 (exigences applicables aux P.S.C. qualifiés), 27, § 4 (signatures électroniques dans les services publics), 28, § 6 (certificats qualifiés de signature électronique), 29, § 2 (dispositifs de création de signature électronique qualifiés), 32, § 3 (validation des signatures électronique qualifiées), 33, § 2 (services de validation qualifié des signatures électroniques qualifiées), 34, § 2 (services de conservation qualifié des signature électroniques qualifiées), 37, § 4 (cachets électroniques dans les services publics), 38, § 6 (certificats qualifiés de cachet électronique), 42, § 2 (établissement du lien entre la date et l'heure et les données, et les horloges exactes, en matière d'horodatage électronique), 44, § 2 (processus d'envoi et de réception des données en matière de service d'envoi recommandé électronique) et 45, § 2 (certificats qualifiés d'authentification de sites internet).
122. Art. 25, § 1er, du règlement.
123. Art. 35, § 1er, du règlement.
124. Art. 41, § 1er, du règlement.
125. Art. 43, § 1er, du règlement.

Cela signifie que l'effet juridique ou la recevabilité de ces services de confiance comme preuve en justice ne peuvent pas être refusés au seul motif qu'ils se présentent sous une forme électronique ou qu'ils ne satisfont pas aux exigences du service de confiance qualifié correspondant.

37. Clause d'assimilation ou présomption pour les services de confiance qualifiés. Les services de confiance qualifiés bénéficient du principe d'assimilation ou d'une présomption légale ayant pour effet de renverser la charge de la preuve.

Aux termes de l'article 25, § 2, du règlement, « l'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite ». *A priori*, le juge ne dispose d'aucune marge d'appréciation et il doit assimiler le procédé à une signature manuscrite. D'après nous, il doit rester possible d'administrer la preuve contraire.

Pour d'autres services de confiance, le règlement présume – de manière réfragable – que les fonctions reconnues à la formalité (et expressément mentionnées) sont atteintes. Tel est le cas pour le cachet électronique qualifié[126] (présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié), l'horodatage électronique qualifié[127] (présomption d'exactitude de la date et de l'heure qu'il indique d'intégrité des données auxquelles se rapportent cette date et cette heure), le service d'envoi recommandé électronique qualifié[128] (présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et à leur réception par le destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées par le service d'envoi recommandé électronique qualifié). Pour le cas plus particulier de l'authentification de site internet, aucune présomption n'est établie.

Qu'en est-il des services de confiance qui ne sont pas qualifiés (et qui ne bénéficient donc pas de la clause d'assimilation ou de la présomption) ?

Sous peine de méconnaître le principe de non-discrimination consacré par ailleurs (et qui interdit de priver d'effet juridique les services de confiance qui ne sont pas qualifiés), il faut admettre que les parties utilisatrices aient la possibilité de démontrer que la signature, le cachet, l'horodatage ou le service d'envoi recommandé respectent les fonctions reconnues à chaque procédé, de manière à convaincre le juge de leur donner des effets juridiques sur le plan probatoire.

126. Art. 35, § 2, du règlement.
127. Art. 41, § 2, du règlement.
128. Art. 43, § 2, du règlement.

Les États membres retrouvent sur ce point leur marge de manœuvre de manière à préciser les fonctions attendues de chaque formalité[129]. Pour la signature électronique, par exemple, c'est le rôle joué par l'article 1322, alinéa 2, du Code civil et on peut supposer qu'il sera conservé par le législateur.

Peut-être introduira-t-il des dispositions comparables pour les autres services de confiance. La démarche ne nous paraît toutefois pas indispensable dans la mesure où, contrairement à la signature, le règlement veille à indiquer clairement les fonctions attendues de ces services dans la définition qui leur est donnée. Une clause transversale générale indiquant qu'il incombe à la partie utilisatrice de démontrer que les fonctions ainsi énoncées sont remplies pour bénéficier des effets sur le plan probatoire (ou autre, le cas échéant), devrait être suffisante.

On note encore que la signature électronique avancée et le cachet électronique avancé peuvent être reconnus, moyennant certaines conditions, si un État membre exige ce type de signature (le cas échéant qui repose sur un certificat qualifié) pour utiliser un service en ligne offert par un organisme du secteur public ou pour l'utiliser au nom de cet organisme[130]. *A fortiori*, dans ce cas, les signatures ou cachets électroniques présentant un niveau de sécurité plus élevé (tels que la signature ou le cachet électroniques qualifiés) se voient reconnaître les mêmes effets. Cette disposition tend à compliquer le régime mis en place (puisqu'il crée une autre catégorie de signature électronique): le considérant n° 50 du règlement le justifie cependant par le fait que «les autorités compétentes dans les États membres utilisent actuellement différents formats de signature électronique avancée pour signer électroniquement leurs documents».

38. Responsabilité. Aux termes de l'article 13, § 1er, du règlement, «[...] les prestataires de service de confiance sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le présent règlement».

Le règlement instaure un régime probatoire plus favorable aux parties utilisatrices de services fournis par des P.S.C. qualifiés puisque, dans ce cas, le prestataire est présumé avoir agi intentionnellement ou par négligence[131]. Pour les autres prestataires, c'est le droit commun qui s'applique et il incombe à la victime de prouver que le prestataire a agi intentionnellement ou par négligence[132].

129. S'agissant de la signature, voy. le considérant n° 49: «il appartient au droit national de définir l'effet juridique produit par les signatures électroniques, à l'exception de l'exigence prévue dans le présent règlement selon laquelle l'effet juridique d'une signature électronique qualifiée devrait être équivalent à celui d'une signature manuscrite».
130. Art. 27 et 37 du règlement.
131. Art. 13, § 1er, al. 3, du règlement.

On note qu'il est permis aux prestataires de services de confiance de poser des limites à l'utilisation des services fournis (indiquer par exemple que le service de signature ou d'horodatage électronique n'est pas garanti pour des montants supérieurs à 1.000.000 euros ou dans certaines matières – comme des paiements). Cette limite – et l'exonération limitative de responsabilité qui en découle – sera étroitement liée aux garanties obtenues par les prestataires auprès de leurs compagnies d'assurance (tenant compte des risques financiers qu'ils sont prêts à assumer)[133]. Encore faut-il, comme le rappelle l'article 13, § 2, du règlement, que les clients soient dûment informés, au préalable, de telles limites, et qu'elles puissent être reconnues par des tiers.

39. Reconnaissance mutuelle au sein de l'Union. Parmi les objectifs du règlement figure le bon fonctionnement du marché intérieur. Il doit se traduire par une libre prestation des services de confiance sur le territoire de l'Union (dans le chef des prestataires qui les fournissent et des parties utilisatrices qui y recourent). Concrètement, il faut permettre à un client belge qui conclut un contrat avec une entreprise française d'utiliser un procédé d'horodatage électronique fourni par une entreprise finlandaise.

En ce sens, le règlement consacre un principe de reconnaissance mutuelle de certains services de confiance qualifiés. Il énonce ainsi que «la signature électronique qualifiée qui repose sur un certificat qualifié délivré dans un État membre est reconnue en tant que signature électronique qualifiée dans tous les États membres»[134]. Des clauses similaires sont introduites pour les cachets électroniques qualifiés[135] et l'horodatage électronique qualifié[136]. Curieusement, rien n'est prévu pour le service d'envoi recommandé électronique qualifié ou la délivrance de certificats qualifiés d'authentification de sites internet.

Qu'en est-il des services de confiance non-qualifiés ou des deux services de confiance qualifiés qui ne bénéficient pas de la clause de reconnaissance mutuelle? Le principe de marché intérieur tel que consacré à l'article 4 du règlement leur est applicable. En son paragraphe 1er, cette disposition interdit, en effet, de restreindre «la fourniture de services de confiance, sur le territoire d'un État membre, par un prestataire établi dans un autre État membre, pour des raisons qui relèvent des domaines couverts par le présent règlement». Quant au paragraphe 2, il autorise

132. Art. 13, § 1er, al. 2, du règlement.
133. Sur ce point, voy. le considérant n° 37 du règlement.
134. Art. 25, § 3, du règlement.
135. Art. 35, § 3, du règlement.
136. Art. 41, § 3, du règlement.

les services de confiance conformes au règlement à circuler librement au sein du marché intérieur.

Conclusion

40. Cadre normatif en évolution. Les dispositions légales ou réglementaires permettant de lever les obstacles à l'accomplissement, dans l'environnement numérique, des principales exigences de forme (écrit, signature, mentions manuscrites, exemplaires multiples, etc.) sont en vigueur depuis le début des années 2000.

En pratique, leur application ne semble pas poser de grandes difficultés, au vu notamment des très rares décisions de jurisprudence rendues à ce propos. L'explication réside peut-être dans la circonstance que ces dispositions ne sont, tout simplement, pas appliquées. Exception faite des paiements, rares sont en effet les procédés de signature électronique réellement utilisés (sans que cela semble poser de problème dans la vie des affaires). Du reste, pour obvier toute difficulté, les parties exploitent le caractère supplétif des règles de preuve pour se dispenser d'exigences trop rigoureuses en terme d'écrit électronique ou d'équivalents fonctionnels aux mentions manuscrites.

Des incertitudes existaient, par contre, concernant les services accessoires à ces formalités principales : horodatage, archivage et recommandé électronique.

Pour y répondre, et instaurer ainsi un climat de confiance propice au développement du commerce électronique, le règlement eIDAS a été adopté.

41. Règlement eIDAS. De manière générale, le règlement doit être approuvé, en ce qu'il renforce la sécurité juridique concernant les services de confiance (sous réserve néanmoins des services d'archivage électronique, dont on regrette l'absence de cadre normatif au niveau européen).

Il faut toutefois reconnaître que le régime mis en place est parfois très complexe (et peu lisible). Il fait aussi la part belle aux prestataires de service de confiance qualifiés et aux services de confiance qualifiés, même si l'on peut craindre qu'au final, les prestataires intéressés restent très rares.

C'est donc le développement des services non-qualifiés qui doit être promu puisqu'en pratique, ce sont eux qui devraient normalement être les plus nombreux. Or, seules quelques dispositions du règlement leur sont applicables. Une plus grande flexibilité est ainsi permise, même si on peut craindre que la sécurité juridique soit parfois compromise.